P7_TA-PROV(2014)0230

US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights

European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))

The European Parliament,

– having regard to the Treaty on European Union (TEU), in particular Articles 2, 3, 4, 5, 6, 7, 10, 11 and 21 thereof,

– having regard to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 15, 16 and 218 and Title V thereof,

– having regard to Protocol 36 on transitional provisions and Article 10 thereof and to Declaration 50 concerning this protocol,

– having regard to the Charter on Fundamental Rights of the European Union, in particular Articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 and 52 thereof,

– having regard to the European Convention on Human Rights, notably Articles 6, 8, 9, 10 and 13 thereof, and the protocols thereto,

– having regard to the Universal Declaration of Human Rights, notably Articles 7, 8, 10,11,12 and 14 thereof[1],

– having regard to the International Covenant on Civil and Political Rights, notably Articles 14, 17, 18 and 19 thereof,

– having regard to the Council of Europe Convention on Data Protection (ETS No 108) and the Additional Protocol of 8 November 2001 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181),

– having regard to the Vienna Convention on Diplomatic Relations, notably Articles 24, 27 and 40 thereof,

– having regard to the Council of Europe Convention on Cybercrime (ETS No 185),

– having regard to the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, submitted on 17 May 2010[2],

---

1 http://www.un.org/en/documents/udhr/

– having regard to the Commission communication on 'Internet Policy and Governance – Europe's role in shaping the future of Internet Governance' (COM(2014)0072);

– having regard to the report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted on 17 April 2013[3],

– having regard to the Guidelines on human rights and the fight against terrorism adopted by the Committee of Ministers of the Council of Europe on 11 July 2002,

– having regard to the Declaration of Brussels of 1 October 2010, adopted at the 6th Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States,

– having regard to Council of Europe Parliamentary Assembly Resolution No 1954 (2013) on national security and access to information,

– having regard to the report on the democratic oversight of the security services adopted by the Venice Commission on 11 June 2007[4], and expecting with great interest the update thereof, due in spring 2014,

– having regard to the testimonies of the representatives of the oversight committees on intelligence of Belgium, the Netherlands, Denmark and Norway,

– having regard to the cases lodged before the French[5], Polish and British[6] courts, as well as before the European Court of Human Rights[7], in relation to systems of mass surveillance,

– having regard to the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union[8], and in particular to Title III thereof,

– having regard to Commission Decision 2000/520/EC of 26 July 2000 on the adequacy of the protection provided by the Safe Harbour privacy principles and the related frequently asked questions (FAQs) issued by the US Department of Commerce,

---

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 and La Ligue française pour la défense des droits de l'Homme et du Citoyen v. X; Tribunal de Grande Instance of Paris.

6 Cases by Privacy International and Liberty in the Investigatory Powers Tribunal.

7 Joint Application Under Article 34 of Big Brother Watch, Open Rights Group, English PEN and Dr Constanze Kurz (applicants) v. United Kingdom (respondent).

8 OJ C 197, 12.7.2000, p. 1.

– having regard to the Commission's assessment reports on the implementation of the Safe Harbour privacy principles of 13 February 2002 (SEC(2002)0196) and of 20 October 2004 (SEC(2004)1323),

– having regard to the Commission communication of 27 November 2013 on the functioning of the Safe Harbour from the perspective of EU citizens and companies established in the EU (COM(2013)0847), and to the Commission communication of 27 November 2013 on rebuilding trust in EU-US data flows (COM(2013)0846),

– having regard to its resolution of 5 July 2000 on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce[9], which took the view that the adequacy of the system could not be confirmed, and to the Opinions of the Article 29 Working Party, more particularly Opinion 4/2000 of 16 May 2000[10],

– having regard to the agreements between the United States of America and the European Union on the use and transfer of passenger name records (PNR agreement) of 2004, 2007[11] and 2012[12],

– having regard to the Joint Review of the implementation of the Agreement between the EU and the USA on the processing and transfer of passenger name records to the US Department of Homeland Security[13], accompanying the report from the Commission to the European Parliament and to the Council on the joint review (COM(2013)0844),

– having regard to the opinion of Advocate General Cruz Villalón concluding that Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks is as a whole incompatible with Article 52(1) of the Charter of Fundamental Rights of the European Union and that Article 6 thereof is incompatible with Articles 7 and 52(1) of the Charter[14],

– having regard to Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (TFTP)[15] and the accompanying declarations by the Commission and the Council,

– having regard to the Agreement on mutual legal assistance between the European Union and the United States of America[16],

– having regard to the ongoing negotiations on an EU-US framework agreement on the protection of personal data when transferred and processed for the purpose of preventing,

---

9 OJ C 121, 24.4.2001, p. 152.
10 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32en.pdf
11 OJ L 204, 4.8.2007, p. 18.
12 OJ L 215, 11.8.2012, p. 5.
13 SEC(2013)0630, 27.11.2013.
14 Opinion of Advocate General Cruz Villalón, 12 December 2013, Case C-293/12.
15 OJ L 195, 27.7.2010, p. 3.
16 OJ L 181, 19.7.2003, p. 34.

investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters (the 'Umbrella agreement'),

– having regard to Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom[17],

– having regard to the statement by the President of the Federative Republic of Brazil at the opening of the 68th session of the UN General Assembly on 24 September 2013 and to the work carried out by the Parliamentary Committee of Inquiry on Espionage established by the Federal Senate of Brazil,

– having regard to the USA PATRIOT Act signed by President George W. Bush on 26 October 2001,

– having regard to the Foreign Intelligence Surveillance Act (FISA) of 1978 and the FISA Amendments Act of 2008,

– having regard to Executive Order No 12333, issued by the US President in 1981 and amended in 2008,

– having regard to the Presidential Policy Directive (PPD-28) on Signals Intelligence Activities, issued by US President Barack Obama on 17 January 2014,

– having regard to legislative proposals currently under examination in the US Congress including the draft US Freedom Act, the draft Intelligence Oversight and Surveillance Reform Act, and others,

– having regard to the reviews conducted by the Privacy and Civil Liberties Oversight Board, the US National Security Council and the President's Review Group on Intelligence and Communications Technology, particularly the report by the latter of 12 December 2013 entitled 'Liberty and Security in a Changing World',

– having regard to the ruling of the United States District Court for the District of Columbia, Klayman et al. v Obama et al., Civil Action No 13-0851 of 16 December 2013, and to the ruling of the United States District Court for the Southern District of New York, ACLU et al. v James R. Clapper et al., Civil Action No 13-3994 of 11 June 2013,

– having regard to the report on the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on data protection of 27 November 2013[18],

– having regard to its resolutions of 5 September 2001[19] and 7 November 2002[20] on the existence of a global system for the interception of private and commercial communications (ECHELON interception system),

---

17 OJ L 309, 29.11.1996, p. 1.

18 Council document 16987/2013.

19 OJ C 72 E, 21.3.2002, p. 221.

20 OJ C 16 E, 22.1.2004, p. 88.

– having regard to its resolution of 21 May 2013 on the EU Charter: standard settings for media freedom across the EU[21],

– having regard to its resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy[22], whereby it instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter

– having regard to working document 1 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights,

– having regard to working document 3 on the relation between the surveillance practices in the EU and the US and the EU data protection provisions,

– having regard to working document 4 on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation,

– having regard to working document 5 on democratic oversight of Member State intelligence services and of EU intelligence bodies,

– having regard to the AFET working document on Foreign Policy Aspects of the Inquiry on Electronic Mass Surveillance of EU Citizens;

– having regard to its resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken[23],

– having regard to its resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance[24],

– having regard to its resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe[25],

– having regard to the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy[26],

– having regard to Annex VIII of its Rules of Procedure,

– having regard to Rule 48 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A7-0139/2014),

The impact of mass surveillance

---

21 Texts adopted, P7_TA(2013)0203.

22 Texts adopted, P7_TA(2013)0322.

23 Texts adopted, P7_TA(2013)0444.

24 Texts adopted, P7_TA(2013)0449.

25 Texts adopted, P7_TA(2013)0535.

26 OJ C 353 E, 3.12.2013, p. 156.

A. whereas data protection and privacy are fundamental rights; whereas security measures, including counterterrorism measures, must therefore be pursued through the rule of law and must be subject to fundamental rights obligations, including those relating to privacy and data protection;

B. whereas information flows and data, which today dominate everyday life and are part of any person's integrity, need to be as secure from intrusion as private homes;

C. whereas the ties between Europe and the United States of America are based on the spirit and principles of democracy, the rule of law, liberty, justice and solidarity;

D. whereas cooperation between the US and the European Union and its Member States in counter-terrorism remains vital for the security and safety of both partners;

E. whereas mutual trust and understanding are key factors in the transatlantic dialogue and partnership;

F. whereas following 11 September 2001, the fight against terrorism became one of the top priorities of most governments; whereas the revelations based on documents leaked by the former NSA contractor Edward Snowden put political leaders under the obligation to address the challenges of overseeing and controlling intelligence agencies in surveillance activities and assessing the impact of their activities on fundamental rights and the rule of law in a democratic society;

G. whereas the revelations since June 2013 have caused numerous concerns within the EU as to:

- the extent of the surveillance systems revealed both in the US and in EU Member States;

- the violation of EU legal standards, fundamental rights and data protection standards;

- the degree of trust between the EU and the US as transatlantic partners;

- the degree of cooperation and involvement of certain EU Member States with US surveillance programmes or equivalent programmes at national level as unveiled by the media;

- the lack of control and effective oversight by the US political authorities and certain EU Member States over their intelligence communities;

- the possibility of these mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense, for example economic and industrial espionage or profiling on political grounds;

- the undermining of press freedom and of communications of members of professions with a confidentiality privilege, including lawyers and doctors;

- the respective roles and degree of involvement of intelligence agencies and private IT and telecom companies;

– the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect and being subject to surveillance;

– the threats to privacy in a digital era and the impact of mass surveillance on citizens and societies;

H. whereas the unprecedented magnitude of the espionage revealed requires full investigation by the US authorities, the European institutions and Member States' governments, national parliaments and judicial authorities;

I. whereas the US authorities have denied some of the information revealed but have not contested the vast majority of it; whereas the public debate has developed on a large scale in the US and in certain EU Member States; whereas EU governments and parliaments too often remain silent and fail to launch adequate investigations;

J. whereas President Obama has recently announced a reform of the NSA and its surveillance programmes;

K. whereas in comparison to actions taken both by EU institutions and by certain EU Member States, the European Parliament has taken very seriously its obligation to shed light on the revelations on the indiscriminate practices of mass surveillance of EU citizens and, by means of its resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens, instructed its Committee on Civil Liberties, Justice and Home Affairs to conduct an in-depth inquiry into the matter;

L. whereas it is the duty of the European institutions to ensure that EU law is fully implemented for the benefit of European citizens and that the legal force of the EU Treaties is not undermined by a dismissive acceptance of extraterritorial effects of third countries' standards or actions;

Developments in the US on reform of intelligence

M. whereas the District Court for the District of Columbia, in its Decision of 16 December 2013, has ruled that the bulk collection of metadata by the NSA is in breach of the Fourth Amendment to the US Constitution[27]; whereas, however the District Court for the Southern District of New York ruled in its Decision of 27 December 2013 that this collection was lawful;

N. whereas a Decision of the District Court for the Eastern District of Michigan has ruled that the Fourth Amendment requires reasonableness in all searches, prior warrants for any reasonable search, warrants based upon prior-existing probable cause, as well as particularity as to persons, place and things and the interposition of a neutral magistrate between executive branch enforcement officers and citizens[28];

O. whereas in its report of 12 December 2013, the President's Review Group on Intelligence and Communication Technology proposes 46 recommendations to the

---

27 Klayman et al. v Obama et al., Civil Action No 13-0851, 16 December 2013.

28 ACLU v. NSA No 06-CV-10204, 17 August 2006.

President of the United States; whereas the recommendations stress the need simultaneously to protect national security and personal privacy and civil liberties; whereas in this regard it invites the US Government: to end bulk collection of phone records of US persons under Section 215 of the USA PATRIOT Act as soon as practicable; to undertake a thorough review of the NSA and the US intelligence legal framework in order to ensure respect for the right to privacy; to end efforts to subvert or make vulnerable commercial software (backdoors and malware); to increase the use of encryption, particularly in the case of data in transit, and not to undermine efforts to create encryption standards; to create a Public Interest Advocate to represent privacy and civil liberties before the Foreign Intelligence Surveillance Court; to confer on the Privacy and Civil Liberties Oversight Board the power to oversee Intelligence Community activities for foreign intelligence purposes, and not only for counterterrorism purposes; and to receive whistleblowers' complaints, to use Mutual Legal Assistance Treaties to obtain electronic communications, and not to use surveillance to steal industry or trade secrets;

P. whereas, according to an open memorandum submitted to President Obama by Former NSA Senior Executives/Veteran Intelligence Professionals for Sanity (VIPS) on 7 January 2014[29], the massive collection of data does not enhance the ability to prevent future terrorist attacks; whereas the authors stress that mass surveillance conducted by the NSA has resulted in the prevention of zero attacks and that billions of dollars have been spent on programmes which are less effective and vastly more intrusive on citizens' privacy than an in-house technology called THINTHREAD that was created in 2001;

Q. whereas in respect of intelligence activities concerning non-US persons under Section 702 of FISA, the Recommendations to the President of the USA recognise the fundamental principle of respect for privacy and human dignity as enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights; whereas they do not recommend granting non-US persons the same rights and protections as US persons;

R. whereas in his Presidential Policy Directive on Signals Intelligence Activities of 17 January 2014 and the related speech, US President Barack Obama stated that mass electronic surveillance is necessary for the United States to protect its national security, its citizens and the citizens of US allies and partners, as well as to advance its foreign policy interests; whereas this policy directive contains certain principles regarding the collection, use and sharing of signals intelligence and extends certain safeguards to non-US persons, partly providing for treatment equivalent to that enjoyed by US citizens, including safeguards for the personal information of all individuals regardless of their nationality or residence; whereas, however, President Obama did not call for any concrete proposals, particularly regarding the prohibition of mass surveillance activities and the introduction of administrative and judicial redress for non-US persons;

Legal framework

Fundamental rights

---

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

S. whereas the report on the findings by the EU Co-Chairs of the ad hoc EU-US Working Group on data protection provides for an overview of the legal situation in the US, but has failed to establish the facts about US surveillance programmes; whereas no information has been made available about the so-called 'second track' Working Group, under which Member States discuss bilaterally with the US authorities matters related to national security;

T. whereas fundamental rights, notably freedom of expression, of the press, of thought, of conscience, of religion and of association, private life, data protection, as well as the right to an effective remedy, the presumption of innocence and the right to a fair trial and non-discrimination, as enshrined in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights, are cornerstones of democracy; whereas mass surveillance of human beings is incompatible with these cornerstones;

U. whereas in all Member States the law protects from disclosure information communicated in confidence between lawyer and client, a principle which has been recognised by the European Court of Justice[30];

V. whereas in its resolution of 23 October 2013 on organised crime, corruption and money laundering Parliament called on the Commission to submit a legislative proposal establishing an effective and comprehensive European whistleblower protection programme in order to protect EU financial interests and furthermore conduct an examination on whether such future legislation should also cover other fields of Union competence;

Union competences in the field of security

W. whereas according to Article 67(3) TFEU the EU 'shall endeavour to ensure a high level of security'; whereas the provisions of the Treaty (in particular Article 4(2) TEU, Article 72 TFEU and Article 73 TFEU) imply that the EU possesses certain competences on matters relating to the collective security of the Union; whereas the EU has competence in matters of internal security (Article 4(j) TFEU) and has exercised this competence by deciding on a number of legislative instruments and concluding international agreements (PNR, TFTP) aimed at fighting serious crime and terrorism, and by setting up an internal security strategy and agencies working in this field;

X. whereas the Treaty on the Functioning of the European Union states that 'it shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security' (Article 73 TFEU);

Y. whereas Article 276 TFEU states that 'in exercising its powers regarding the provisions of Chapters 4 and 5 of Title V of Part Three relating to the area of freedom, security and justice, the Court of Justice of the European Union shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law enforcement services of a Member State or the exercise of the responsibilities

---

[30] Judgement of 18 May 1982 in Case C-155/79, AM & S Europe Limited v Commission of the European Communities.

incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security';

Z. whereas the concepts of 'national security', 'internal security', 'internal security of the EU' and 'international security' overlap; whereas the Vienna Convention on the Law of Treaties, the principle of sincere cooperation among EU Member States and the human rights law principle of interpreting any exemptions narrowly point towards a restrictive interpretation of the notion of 'national security' and require that Member States refrain from encroaching upon EU competences;

AA. whereas the European Treaties confer on the European Commission the role of the 'Guardian of the Treaties', and it is therefore the legal responsibility of the Commission to investigate any potential breaches of EU law;

AB. whereas, in accordance with Article 6 TEU, referring to the EU Charter of Fundamental Rights and the ECHR, Member States' agencies and even private parties acting in the field of national security also have to respect the rights enshrined therein, be they of their own citizens or of citizens of other states;

Extraterritoriality

AC. whereas the extraterritorial application by a third country of its laws, regulations and other legislative or executive instruments in situations falling under the jurisdiction of the EU or its Member States may impact on the established legal order and the rule of law, or even violate international or EU law, including the rights of natural and legal persons, taking into account the extent and the declared or actual aim of such an application; whereas, in these circumstances, it is necessary to take action at Union level to ensure that the EU values enshrined in Article 2 TEU, the Charter of Fundamental Rights, the ECHR referring to fundamental rights, democracy and the rule of law, and the rights of natural and legal persons as enshrined in secondary legislation applying these fundamental principles, are respected within the EU, for example by removing, neutralising, blocking or otherwise countering the effects of the foreign legislation concerned;

International transfers of data

AD. whereas the transfer of personal data by EU institutions, bodies, offices or agencies or by the Member States to the US for law enforcement purposes in the absence of adequate safeguards and protections for the respect of the fundamental rights of EU citizens, in particular the rights to privacy and the protection of personal data, would make that EU institution, body, office or agency or that Member State liable, under Article 340 TFEU or the established case law of the CJEU[31], for breach of EU law – which includes any violation of the fundamental rights enshrined in the EU Charter;

AE. whereas the transfer of data is not geographically limited, and, especially in a context of increasing globalisation and worldwide communication, the EU legislator is confronted with new challenges in terms of protecting personal data and communications; whereas

---

31 See notably Joined Cases C-6/90 and C-9/90, Francovich and others v. Italy, judgment of 28 May 1991.

it is therefore of the utmost importance to foster legal frameworks on common standards;

AF. whereas the mass collection of personal data for commercial purposes and in the fight against terror and serious transnational crime puts at risk the personal data and privacy rights of EU citizens;

Transfers to the US based on the US Safe Harbour

AG. whereas the US data protection legal framework does not ensure an adequate level of protection for EU citizens;

AH. whereas, in order to enable EU data controllers to transfer personal data to an entity in the US, the Commission, in its Decision 2000/520/EC, has declared the adequacy of the protection provided by the Safe Harbour privacy principles and the related FAQs issued by the US Department of Commerce for personal data transferred from the Union to organisations established in the US that have joined the Safe Harbour;

AI. whereas in its resolution of 5 July 2000 Parliament expressed doubts and concerns as to the adequacy of the Safe Harbour, and called on the Commission to review the decision in good time, in the light of experience and of any legislative developments;

AJ. whereas in Parliament's working document 4 on US Surveillance activities with respect to EU data and its possible legal implications on transatlantic agreements and cooperation of 12 December 2013, the rapporteurs expressed doubts and concerns as to the adequacy of Safe Harbour and called on the Commission to repeal the decision on the adequacy of Safe Harbour and to find new legal solutions;

AK. whereas Commission Decision 2000/520/EC stipulates that the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Safe Harbour principles, in order to protect individuals with regard to the processing of their personal data in cases where there is a substantial likelihood that the Safe Harbour principles are being violated or that the continuing transfer would create an imminent risk of grave harm to data subjects;

AL. whereas Commission Decision 2000/520/EC also states that where evidence has been provided that anybody responsible for ensuring compliance with the principles is not effectively fulfilling their role, the Commission must inform the US Department of Commerce and, if necessary, present measures with a view to reversing or suspending the Decision or limiting its scope;

AM. whereas in its first two reports on the implementation of the Safe Harbour, published in 2002 and 2004, the Commission identified several deficiencies as regards the proper implementation of the Safe Harbour and made a number of recommendations to the US authorities with a view to rectifying those deficiencies;

AN. whereas in its third implementation report, of 27 November 2013, nine years after the second report and without any of the deficiencies recognised in that report having been rectified, the Commission identified further wide-ranging weaknesses and shortcomings in the Safe Harbour and concluded that the current implementation could not be maintained; whereas the Commission has stressed that wide-ranging access by US

intelligence agencies to data transferred to the US by Safe Harbour-certified entities raises additional serious questions as to the continuity of protection of the data of EU data subjects; whereas the Commission addressed 13 recommendations to the US authorities and undertook to identify by summer 2014, together with the US authorities, remedies to be implemented as soon as possible, forming the basis for a full review of the functioning of the Safe Harbour principles;

AO. whereas on 28-31 October 2013 a delegation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) met in Washington D.C. with the US Department of Commerce and the US Federal Trade Commission; whereas the Department of Commerce acknowledged the existence of organisations having self-certified adherence to Safe Harbour Principles but clearly showing a 'not-current status', meaning that the company does not fulfil Safe Harbour requirements although continuing to receive personal data from the EU; whereas the Federal Trade Commission admitted that the Safe Harbour should be reviewed in order to improve it, particularly with regard to complaints and alternative dispute resolution systems;

AP. whereas Safe Harbour Principles may be limited 'to the extent necessary to meet national security, public interest, or law enforcement requirements'; whereas, as an exception to a fundamental right, such an exception must always be interpreted restrictively and be limited to what is necessary and proportionate in a democratic society, and the law must clearly establish the conditions and safeguards to make this limitation legitimate; whereas the scope of application of such exception should have been clarified by the US and the EU, notably by the Commission, to avoid any interpretation or implementation that nullifies in substance the fundamental right to privacy and data protection, among others; whereas, consequently, such an exception should not be used in a way that undermines or nullifies the protection afforded by Charter of Fundamental Rights, the ECHR, the EU data protection law and the Safe Harbour principles; insists that if the national security exception is invoked, it must be specified under which national law;

AQ. whereas large-scale access by US intelligence agencies has seriously eroded transatlantic trust and negatively impacted on trust as regards US organisations acting in the EU; whereas this is further exacerbated by the lack of judicial and administrative redress for EU citizens under US law, particularly in cases of surveillance activities for intelligence purposes;

Transfers to third countries with the adequacy decision

AR. whereas according to the information revealed and to the findings of the inquiry conducted by the LIBE Committee, the national security agencies of New Zealand, Canada and Australia have been involved on a large scale in mass surveillance of electronic communications and have actively cooperated with the US under the so-called 'Five Eyes' programme, and may have exchanged with each other personal data of EU citizens transferred from the EU;

AS. whereas Commission Decisions 2013/65/EU[32] and 2002/2/EC[33] have declared the levels of protection ensured by, respectively, the New Zealand Privacy Act and the Canadian

---

32 OJ L 28, 30.1.2013, p. 12.

33 OJ L 2, 4.1.2002, p. 13.

Personal Information Protection and Electronic Documents Act to be adequate; whereas the aforementioned revelations also seriously affect trust in the legal systems of these countries as regards the continuity of protection afforded to EU citizens; whereas the Commission has not examined this aspect;

Transfers based on contractual clauses and other instruments

AT. whereas Directive 95/46/EC provides that international transfers to a third country may also take place by means of specific instruments whereby the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights;

AU. whereas such safeguards may in particular result from appropriate contractual clauses;

AV. whereas Directive 95/46/EC empowers the Commission to decide that specific standard contractual clauses offer sufficient safeguards required by the Directive, and whereas on this basis the Commission has adopted three models of standard contractual clauses for transfers to controllers and processors (and sub-processors) in third countries;

AW. whereas the Commission Decisions establishing the standard contractual clauses stipulate that the competent authorities in Member States may exercise their existing powers to suspend data flows where it is established that the law to which the data importer or a sub-processor is subject imposes upon them requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC, where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or where there is a substantial likelihood that the standard contractual clauses in the annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects;

AX. whereas national data protection authorities have developed binding corporate rules (BCRs) in order to facilitate international transfers within a multinational corporation with adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; whereas before being used, BCRs need to be authorised by the Member States' competent authorities after the latter have assessed compliance with Union data protection law; whereas BCRs for data processors have been rejected in the LIBE Committee report on the General Data Protection Regulation, as they would leave the data controller and the data subject without any control over the jurisdiction in which their data is processed;

AY. whereas the European Parliament, given its competence stipulated by Article 218 TFEU, has the responsibility to continuously monitor the value of international agreements it has given its consent to;

Transfers based on TFTP and PNR agreements

AZ. whereas in its resolution of 23 October 2013 Parliament expressed serious concerns over the revelations concerning the NSA's activities as regards direct access to financial

payments messages and related data, which would constitute a clear breach of the TFTP Agreement, and in particular Article 1 thereof;

BA. whereas terrorist finance tracking is an essential tool in the fight against terrorism financing and serious crime, allowing counterterrorism investigators to discover links between targets of investigation and other potential suspects connected with wider terrorist networks suspected of financing terrorism;

BB. whereas Parliament asked the Commission to suspend the Agreement and requested that all relevant information and documents be made available immediately for Parliament's deliberations; whereas the Commission has done neither;

BC. whereas following the allegations published by the media, the Commission decided to open consultations with the US pursuant to Article 19 of the TFTP Agreement; whereas on 27 November 2013 Commissioner Malmström informed the LIBE Committee that, after meeting US authorities and in view of the replies given by the US authorities in their letters and during their meetings, the Commission had decided not to pursue the consultations on the grounds that there were no elements showing that the US Government has acted in a manner contrary to the provisions of the Agreement, and that the US has provided written assurance that no direct data collection has taken place contrary to the provisions of the TFTP agreement; whereas it is not clear whether the US authorities have circumvented the Agreement by accessing such data through other means, as indicated in the letter of 18 September 2013 from the US authorities[34];

BD. whereas during its visit to Washington of 28-31 October 2013 the LIBE delegation met with the US Department of the Treasury; whereas the US Treasury stated that since the entry into force of the TFTP Agreement it had not had access to data from SWIFT in the EU except within the framework of the TFTP; whereas the US Treasury refused to comment on whether SWIFT data would have been accessed outside TFTP by any other US government body or department or whether the US administration was aware of NSA mass surveillance activities; whereas on 18 December 2013 Mr Glenn Greenwald stated before the inquiry held by the LIBE Committee that the NSA and GCHQ had targeted SWIFT networks;

BE. whereas the Belgian and Netherlands data protection authorities decided on 13 November 2013 to conduct a joint investigation into the security of SWIFT's payment networks in order to ascertain whether third parties could gain unauthorised or unlawful access to European citizens' bank data[35];

BF. whereas according to the Joint Review of the EU-US PNR agreement, the US Department of Homeland Security (DHS) made 23 disclosures of PNR data to the NSA on a case-by-case basis in support of counterterrorism cases, in a manner consistent with the specific terms of the Agreement;

---

34 The letter states that 'the US government seeks and obtains financial information ... [which] is collected through regulatory, law enforcement, diplomatic and intelligence channels, as well as through exchanges with foreign partners' and that 'the US Government is using the TFTP to obtain SWIFT data that we do not obtain from other sources'.

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

BG. whereas the Joint Review fails to mention the fact that in the case of processing of personal data for intelligence purposes, under US law, non-US citizens do not enjoy any judicial or administrative avenue to protect their rights, and constitutional protections are only granted to US persons; whereas this lack of judicial or administrative rights nullifies the protections for EU citizens laid down in the existing PNR agreement;

Transfers based on the EU-US Mutual Legal Assistance Agreement in criminal matters

BH. whereas the EU-US Agreement on mutual legal assistance in criminal matters of 6 June 2003[36] entered into force on 1 February 2010 and is intended to facilitate cooperation between the EU and the US to combat crime in a more effective way, having due regard for the rights of individuals and the rule of law;

Framework agreement on data protection in the field of police and judicial cooperation ('umbrella agreement')

BI. whereas the purpose of this general agreement is to establish the legal framework for all transfers of personal data between the EU and US for the sole purposes of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters; whereas negotiations were authorised by the Council on 2 December 2010; whereas this agreement is of the utmost importance and would act as the basis to facilitate data transfer in the context of police and judicial cooperation and in criminal matters;

BJ. whereas this agreement should provide for clear and precise and legally binding data-processing principles, and should in particular recognise EU citizens' right to judicial access to and rectification and erasure of their personal data in the US, as well as the right to an efficient administrative and judicial redress mechanism for EU citizens in the US and independent oversight of the data-processing activities;

BK. whereas in its communication of 27 November 2013 the Commission indicated that the 'umbrella agreement' should result in a high level of protection for citizens on both sides of the Atlantic and should strengthen the trust of Europeans in EU-US data exchanges, providing a basis on which to develop EU-US security cooperation and partnership further;

BL. whereas negotiations on the agreement have not progressed because of the US Government's persistent position of refusing recognition of effective rights of administrative and judicial redress to EU citizens and because of the intention of providing broad derogations to the data protection principles contained in the agreement, such as purpose limitation, data retention or onward transfers either domestically or abroad;

Data protection reform

BM. whereas the EU data protection legal framework is currently being reviewed in order to establish a comprehensive, consistent, modern and robust system for all data-processing activities in the Union; whereas in January 2012 the Commission presented a package

---

[36] OJ L 181, 19.7.2003, p. 25.

of legislative proposals: a General Data Protection Regulation[37], which will replace Directive 95/46/EC and establish a uniform law throughout the EU, and a Directive[38] which will lay down a harmonised framework for all data processing activities by law enforcement authorities for law enforcement purposes and will reduce the current divergences among national laws;

BN. whereas on 21 October 2013 the LIBE Committee adopted its legislative reports on the two proposals and a decision on the opening of negotiations with the Council with a view to having the legal instruments adopted during this legislative term;

BO. whereas, although the European Council of 24/25 October 2013 called for the timely adoption of a strong EU General Data Protection framework in order to foster the trust of citizens and businesses in the digital economy, after two years of deliberations the Council has still been unable to arrive at a general approach on the General Data Protection Regulation and the Directive[39];

IT security and cloud computing

BP. whereas Parliament's abovementioned resolution of 10 December 2013 emphasises the economic potential of 'cloud computing' business for growth and employment; whereas the overall economic value of the cloud market is forecast to be worth USD 207 billion a year by 2016, or twice its value in 2012;

BQ. whereas the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context; whereas Union data protection law, since it is technologically neutral, already applies fully to cloud computing services operating in the EU;

BR. whereas mass surveillance activities give intelligence agencies access to personal data stored or otherwise processed by EU individuals under cloud services agreements with major US cloud providers; whereas the US intelligence authorities have accessed personal data stored or otherwise processed in servers located on EU soil by tapping into the internal networks of Yahoo and Google; whereas such activities constitute a violation of international obligations and of European fundamental rights standards including the right to private and family life, the confidentiality of communications, the presumption of innocence, freedom of expression, freedom of information, freedom of assembly and association and the freedom to conduct business; whereas it is not excluded that information stored in cloud services by Member States' public authorities or undertakings and institutions has also been accessed by intelligence authorities;

BS. whereas US intelligence agencies have a policy of systematically undermining cryptographic protocols and products in order to be able to intercept even encrypted communication; whereas the US National Security Agency has collected vast numbers of so called 'zero-day exploits' – IT security vulnerabilities that are not yet known to the public or the product vendor; whereas such activities massively undermine global efforts to improve IT security;

---

37 COM(2012)0011, 25.1.2012.

38 COM(2012)0010, 25.1.2012.

39 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf

BT. whereas the fact that intelligence agencies have accessed personal data of users of online services has severely distorted the trust of citizens in such services, and therefore has an adverse effect on businesses investing in the development of new services using 'Big Data' and new applications such as the 'Internet of Things';

BU. whereas IT vendors often deliver products that have not been properly tested for IT security or that even sometimes have backdoors implanted purposefully by the vendor; whereas the lack of liability rules for software vendors has led to such a situation, which is in turn exploited by intelligence agencies but also leaves open the risk of attacks by other entities;

BV. whereas it is essential for companies providing such new services and applications to respect the data protection rules and privacy of the data subjects whose data are collected, processed and analysed, in order to maintain a high level of trust among citizens;

Democratic oversight of intelligence services

BW. whereas intelligence services in democratic societies are given special powers and capabilities to protect fundamental rights, democracy and the rule of law, citizens' rights and the State against internal and external threats, and are subject to democratic accountability and judicial oversight; whereas they are given special powers and capabilities only to this end; whereas these powers should be used within the legal limits imposed by fundamental rights, democracy and the rule of law and their application should be strictly scrutinised, as otherwise they lose legitimacy and risk undermining democracy;

BX. whereas the fact that a certain level of secrecy is conceded to intelligence services in order to avoid endangering ongoing operations, revealing modi operandi or putting at risk the lives of agents, such secrecy cannot override or exclude rules on democratic and judicial scrutiny and examination of their activities, as well as on transparency, notably in relation to the respect of fundamental rights and the rule of law, all of which are cornerstones in a democratic society;

BY. whereas most of the existing national oversight mechanisms and bodies were set up or revamped in the 1990s and have not necessarily been adapted to the rapid political and technological developments over the last decade that have led to increased international intelligence cooperation, also through the large scale exchange of personal data, and often blurring the line between intelligence and law enforcement activities;

BZ. whereas democratic oversight of intelligence activities is still only conducted at national level, despite the increase in exchange of information between EU Member States and between Member States and third countries; whereas there is an increasing gap between the level of international cooperation on the one hand and oversight capacities limited to the national level on the other, which results in insufficient and ineffective democratic scrutiny;

CA. whereas national oversight bodies often do not have full access to intelligence received from a foreign intelligence agency, which can lead to gaps in which international information exchanges can take place without adequate review; whereas this problem is further aggravated by the so-called 'third party rule' or the principle of 'originator

control', which has been designed to enable originators to maintain control over the further dissemination of their sensitive information, but is unfortunately often interpreted as applying also to the recipient services' oversight;

CB. whereas private and public transparency reform initiatives are key to ensuring public trust in the activities of intelligence agencies; whereas legal systems should not prevent companies from disclosing to the public information about how they handle all types of government requests and court orders for access to user data, including the possibility of disclosing aggregate information on the number of requests and orders approved and rejected;

Main findings

1. Considers that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, admissions by authorities, and the insufficient response to these allegations, have resulted in compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner;

2. Points specifically to US NSA intelligence programmes allowing for the mass surveillance of EU citizens through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted 'man-in-the-middle attacks' on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme);

3. Notes the allegations of 'hacking' or tapping into the Belgacom systems by the UK intelligence agency GCHQ; notes the statements by Belgacom that it could neither confirm nor deny that EU institutions were targeted or affected, and that the malware used was extremely complex and its development and use would require extensive financial and staffing resources that would not be available to private entities or hackers;

4. Emphasises that trust has been profoundly shaken: trust between the two transatlantic partners, trust between citizens and their governments, trust in the functioning of democratic institutions on both sides of the Atlantic, trust in the respect of the rule of law, and trust in the security of IT services and communication; believes that in order to rebuild trust in all these dimensions, an immediate and comprehensive response plan comprising a series of actions which are subject to public scrutiny is needed;

5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are

incompatible with the principles of necessity and proportionality in a democratic society;

6. Recalls the EU's firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection;

7. Considers that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled;

8. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Titles I and VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4(3) of the Treaty on European Union, as well as the principle that Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives';

9. Notes that international treaties and EU and US legislation, as well as national oversight mechanisms, have failed to provide for the necessary checks and balances or for democratic accountability;

10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws;

11. Considers it crucial that the professional confidentiality privilege of lawyers, journalists, doctors and other regulated professions is safeguarded against mass surveillance activities; stresses, in particular, that any uncertainty about the confidentiality of communications between lawyers and their clients could negatively impact on EU citizens' right of access to legal advice and access to justice and the right to a fair trial;

12. Sees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence;

recalls in this regard the decision of the German Federal Constitutional Court[40] on the prohibition of the use of preventive dragnets ('präventive Rasterfahndung') unless there is proof of a concrete danger to other high-ranking legally protected rights, whereby a general threat situation or international tensions do not suffice to justify such measures;

13. Is convinced that secret laws and courts violate the rule of law; points out that any judgment of a court or tribunal and any decision of an administrative authority of a non-EU state authorising, directly or indirectly, the transfer of personal data, may not be recognised or enforced in any manner unless there is a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State and a prior authorisation by the competent supervisory authority; recalls that any judgment of a secret court or tribunal and any decision of an administrative authority of a non-EU state secretly authorising, directly or indirectly, surveillance activities shall not be recognised or enforced;

14. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments, since internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data; considers that the scale of this problem is unprecedented; notes that this may create a situation where infrastructure for the mass collection and processing of data could be misused in cases of change of political regime;

15. Notes that there is no guarantee, either for EU public institutions or for citizens, that their IT security or privacy can be protected from attacks by well-equipped intruders ('no 100 % IT security'); notes that in order to achieve maximum IT security, Europeans need to be willing to dedicate sufficient resources, both human and financial, to preserving Europe's independence and self-reliance in the field of IT;

16. Strongly rejects the notion that all issues related to mass surveillance programmes are purely a matter of national security and therefore the sole competence of Member States; reiterates that Member States must fully respect EU law and the ECHR while acting to ensure their national security; recalls a recent ruling of the Court of Justice according to which 'although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable'[41]; recalls further that the protection of the privacy of all EU citizens is at stake, as are the security and reliability of all EU communication networks; believes, therefore, that discussion and action at EU level are not only legitimate, but also a matter of EU autonomy;

17. Commends the institutions and experts who have contributed to this Inquiry; deplores the fact that several Member States' authorities have declined to cooperate with the inquiry the European Parliament has been conducting on behalf of citizens; welcomes the openness of several Members of Congress and of national parliaments;

18. Is aware that in such a limited timeframe it has been possible to conduct only a preliminary investigation of all the issues at stake since July 2013; recognises both the scale of the revelations involved and their ongoing nature; adopts, therefore, a forward-

---

40 No 1 BvR 518/02 of 4 April 2006.

41 Judgement in Case C-300/11, ZZ v Secretary of State for the Home Department, 4 June 2013.

planning approach consisting in a set of specific proposals and a mechanism for follow-up action in the next parliamentary term, ensuring the findings remain high on the EU political agenda;

19. Intends to request strong political undertakings from the new Commission which will be designated after the May 2014 European elections to the effect that it will implement the proposals and recommendations of this Inquiry;

Recommendations

20. Calls on the US authorities and the EU Member States, where this is not yet the case, to prohibit blanket mass surveillance activities;

21. Calls on the EU Member States, and in particular those participating in the so-called '9-eyes' and '14-eyes' programmes[42], to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny, that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency, including by reference to the UN compilation of good practices and the recommendations of the Venice Commission, and that they are in line with the standards of the European Convention on Human Rights and comply with Member States' fundamental rights obligations, in particular as regards data protection, privacy, and the presumption of innocence;

22. Calls on all EU Member States and in particular, with regard to its Resolution of 4 July 2013 and Inquiry Hearings, the United Kingdom, France, Germany, Sweden, the Netherlands and Poland to ensure that their current or future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies are in line with the standards of the European Convention on Human Rights and European Union data protection legislation; calls on these Member States to clarify the allegations of mass surveillance activities, including mass surveillance of cross border telecommunications, untargeted surveillance on cable-bound communications, potential agreements between intelligence services and telecommunication companies as regards access and exchange of personal data and access to transatlantic cables, US intelligence personnel and equipment on EU territory without oversight on surveillance operations, and their compatibility with EU legislation; invites the national parliaments of those countries to intensify cooperation of their intelligence oversight bodies at European level;

23. Calls on the United Kingdom, in particular, given the extensive media reports referring to mass surveillance by the intelligence service GCHQ, to revise its current legal framework, which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers Act 2000;

24. Takes note of the review of the Dutch Intelligence and Security Act 2002 (report by the Dessens Commission of 2 December 2013); supports those recommendations of the review commission which aim to strengthen the transparency, control and oversight of

---

42 The '9-eyes programme' comprises the US, the UK, Canada, Australia, New Zealand, Denmark, France, Norway and the Netherlands; the '14-eyes programme' includes those countries and also Germany, Belgium, Italy, Spain and Sweden.

the Dutch intelligence services; calls on the Netherlands to refrain from extending the powers of the intelligence services in such a way as to enable untargeted and large-scale surveillance also to be performed on cable-bound communications of innocent citizens, especially given the fact that one of the biggest Internet Exchange Points in the world is located in Amsterdam (AMS-IX); calls for caution in defining the mandate and capabilities of the new Joint Sigint Cyber Unit, as well as for caution regarding the presence and operation of US intelligence personnel on Dutch territory;

25. Calls on the Member States, including when represented by their intelligence agencies, to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including the protection of human rights under the TEU, the ECHR and the EU Charter of Fundamental Rights;

26. Calls for the termination of mass interception and processing of webcam imagery by any secret service; calls upon the Member States to fully investigate whether, how and to what extent their respective secret services have been involved in the collection and processing of webcam images, and to delete all stored images collected through such mass surveillance programmes;

27. Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law;

28. Invites the Secretary-General of the Council of Europe to launch the Article 52 procedure according to which 'on receipt of a request from the Secretary-General of the Council of Europe any High Contracting Party shall furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention';

29. Calls on Member States to take appropriate action immediately, including court action, against the breach of their sovereignty, and thereby the violation of general public international law, perpetrated through the mass surveillance programmes; calls further on Member States to make use of all available international measures to defend EU citizens' fundamental rights, notably by triggering the inter-state complaint procedure under Article 41 of the International Covenant on Civil and Political Rights (ICCPR);

30. Calls upon the Member States to establish effective mechanisms whereby those responsible for (mass) surveillance programmes that are in violation of the rule of law and the fundamental rights of citizens are held accountable for this abuse of power;

31. Calls on the US to revise its legislation without delay in order to bring it into line with international law, to recognise the privacy and other rights of EU citizens, to provide for judicial redress for EU citizens, to put rights of EU citizens on an equal footing with rights of US citizens, and to sign the Optional Protocol allowing for complaints by individuals under the ICCPR;

32. Welcomes, in this regard, the remarks made and the Presidential Policy Directive issued by US President Obama on 17 January 2014, as a step towards limiting authorisation of the use of surveillance and data processing to national security purposes and towards equal treatment of all individuals' personal information, regardless of their nationality or residence, by the US intelligence community; awaits, however, in the context of the EU-US relationship, further specific steps which will, most importantly, strengthen trust in transatlantic data transfers and provide for binding guarantees for enforceable privacy rights of EU citizens, as outlined in detail in this report;

33. Stresses its serious concerns in relation to the work within the Council of Europe's Cybercrime Convention Committee on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 (Budapest Convention) on transborder access to stored computer data with consent or where publicly available, and opposes any conclusion of an additional protocol or guidance intended to broaden the scope of this provision beyond the current regime established by this Convention, which is already a major exception to the principle of territoriality because it could result in unfettered remote access by law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLA agreements and other instruments of judicial cooperation put in place to guarantee the fundamental rights of the individual, including data protection and due process, and in particular Council of Europe Convention 108;

34. Calls on the Commission to carry out, before July 2014, an assessment of the applicability of Regulation (EC) No 2271/96 to cases of conflict of laws on transfers of personal data;

35. Calls on the Fundamental Rights Agency to undertake in-depth research on the protection of fundamental rights in the context of surveillance, and in particular on the current legal situation of EU citizens with regard to the judicial remedies available to them in relation to those practices;

International transfers of data

US data protection legal framework and US Safe Harbour

36. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by the US NSA are companies that have self-certified their adherence to the Safe Harbour, and that the Safe Harbour is the legal instrument used for the transfer of EU personal data to the US (examples being Google, Microsoft, Yahoo!, Facebook, Apple and LinkedIn); expresses its concerns that these organisations have not encrypted information and communications flowing between their data centres, thereby enabling intelligence services to intercept information; welcomes the subsequent statements by some US companies that they will accelerate plans to implement encryption of data flows between their global data centres;

37. Considers that large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not meet the criteria for derogation under ‘national security’;

38. Takes the view that, as under the current circumstances the Safe Harbour principles do not provide adequate protection for EU citizens, these transfers should be carried out

under other instruments, such as contractual clauses or BCRs, provided these instruments set out specific safeguards and protections and are not circumvented by other legal frameworks;

39. Takes the view that the Commission has failed to act to remedy the well-known deficiencies of the current implementation of Safe Harbour;

40. Calls on the Commission to present measures providing for the immediate suspension of Commission Decision 2000/520/EC, which declared the adequacy of the Safe Harbour privacy principles, and of the related FAQs issued by the US Department of Commerce; calls on the US authorities, therefore, to put forward a proposal for a new framework for transfers of personal data from the EU to the US which meets Union law data protection requirements and provides for the required adequate level of protection;

41. Calls on Member States' competent authorities, in particular the data protection authorities, to make use of their existing powers and immediately suspend data flows to any organisation that has self-certified its adherence to the US Safe Harbour Principles, and to require that such data flows are only carried out under other instruments and provided they contain the necessary safeguards and guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals;

42. Calls on the Commission to present, by December 2014, a comprehensive assessment of the US privacy framework covering commercial, law enforcement and intelligence activities, and concrete recommendations based on the absence of a general data protection law in the US; encourages the Commission to engage with the US administration in order to establish a legal framework providing for a high level of protection of individuals with regard to the protection of their personal data when transferred to the US and ensure the equivalence of EU and US privacy frameworks;

Transfers to other third countries with adequacy decision

43. Recalls that Directive 95/46/EC stipulates that transfers of personal data to a third country may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of the Directive, the third country in question ensures an adequate level of protection, the purpose of this provision being to ensure the continuity of the protection afforded by EU data protection law where personal data are transferred outside the EU;

44. Recalls that Directive 95/46/EC also provides that the adequacy of the level of protection afforded by a third country is to be assessed in the light of all the circumstances surrounding a data transfer operation or set of such operations; recalls likewise that the said Directive also equips the Commission with implementing powers to declare that a third country ensures an adequate level of protection in the light of the criteria laid down by Directive 95/46/EC; recalls that Directive 95/46/EC also empowers the Commission to declare that a third country does not ensure an adequate level of protection;

45. Recalls that in the latter case Member States must take the measures necessary to prevent any transfer of data of the same type to the third country in question, and that the Commission should enter into negotiations with a view to remedying the situation;

46. Calls on the Commission and the Member States to assess without delay whether the adequate level of protection of the New Zealand Privacy Act and of the Canadian Personal Information Protection and Electronic Documents Act, as declared by Commission Decisions 2013/65/EU and 2002/2/EU, has been affected by the involvement of those countries' national intelligence agencies in the mass surveillance of EU citizens, and, if necessary, to take appropriate measures to suspend or reverse the adequacy decisions; also calls on the Commission to assess the situation for other countries that have received an adequacy rating; expects the Commission to report to Parliament on its findings on the above-mentioned countries by December 2014 at the latest;

Transfers based on contractual clauses and other instruments

47. Recalls that national data protection authorities have indicated that neither standard contractual clauses nor BCRs were formulated with situations of access to personal data for mass surveillance purposes in mind, and that such access would not be in line with the derogation clauses of the contractual clauses or BCRs which refer to exceptional derogations for a legitimate interest in a democratic society and where necessary and proportionate;

48. Calls on the Member States to prohibit or suspend data flows to third countries based on the standard contractual clauses, contractual clauses or BCRs authorised by the national competent authorities where it is likely that the law to which data recipients are subject imposes requirements on them which go beyond the restrictions that are strictly necessary, adequate and proportionate in a democratic society and are likely to have an adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses, or because continuing transfer would create a risk of grave harm to the data subjects;

49. Calls on the Article 29 Working Party to issue guidelines and recommendations on the safeguards and protections that contractual instruments for international transfers of EU personal data should contain in order to ensure the protection of the privacy, fundamental rights and freedoms of individuals, taking particular account of the third-country laws on intelligence and national security and the involvement of the companies receiving the data in a third country in mass surveillance activities by a third country's intelligence agencies;

50. Calls on the Commission to examine without delay the standard contractual clauses it has established in order to assess whether they provide the necessary protection as regards access to personal data transferred under the clauses for intelligence purposes and, if appropriate, to review them;

Transfers based on the Mutual Legal Assistance Agreement

51. Calls on the Commission to conduct, before the end of 2014, an in-depth assessment of the existing Mutual Legal Assistance Agreement, pursuant to its Article 17, in order to verify its practical implementation and, in particular, whether the US has made effective use of it for obtaining information or evidence in the EU and whether the Agreement has been circumvented to acquire the information directly in the EU, and to assess the impact on the fundamental rights of individuals; such an assessment should not only refer to US official statements as a sufficient basis for the analysis but also be based on

specific EU evaluations; this in-depth review should also address the consequences of the application of the Union's constitutional architecture to this instrument in order to bring it into line with Union law, taking account in particular of Protocol 36 and Article 10 thereof and Declaration 50 concerning this protocol; calls on the Council and Commission also to assess bilateral agreements between Member States and the US so as to ensure that they are consistent with the agreements that the EU follows or decides to follow with the US;

EU mutual assistance in criminal matters

52. Asks the Council and Commission to inform Parliament about the actual use by Member States of the Convention on Mutual Assistance in Criminal Matters between the Member States, in particular its Title III on interception of telecommunications; calls on the Commission to put forward a proposal, in accordance with Declaration 50, concerning Protocol 36, as requested, before the end of 2014 in order to adapt it to the Lisbon Treaty framework;

Transfers based on the TFTP and PNR agreements

53. Takes the view that the information provided by the European Commission and the US Treasury does not clarify whether US intelligence agencies have access to SWIFT financial messages in the EU by intercepting SWIFT networks or banks' operating systems or communication networks, alone or in cooperation with EU national intelligence agencies and without having recourse to existing bilateral channels for mutual legal assistance and judicial cooperation;

54. Reiterates its resolution of 23 October 2013 and asks the Commission for the suspension of the TFTP Agreement;

55. Calls on the Commission to react to concerns that three of the major computerised reservation systems used by airlines worldwide are based in the US and that PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy;

Framework agreement on data protection in the field of police and judicial cooperation ('Umbrella Agreement')

56. Considers that a satisfactory solution under the 'Umbrella agreement' is a precondition for the full restoration of trust between the transatlantic partners;

57. Asks for an immediate resumption of the negotiations with the US on the 'Umbrella Agreement', which should put rights for EU citizens on an equal footing with rights for US citizens; stresses that, moreover, this agreement should provide effective and enforceable administrative and judicial remedies for all EU citizens in the US without any discrimination;

58. Asks the Commission and Council not to initiate any new sectorial agreements or arrangements for the transfer of personal data for law enforcement purposes with the US as long as the 'Umbrella Agreement' has not entered into force;

59. Urges the Commission to report in detail on the various points of the negotiating mandate and the latest state of play by April 2014;

Data protection reform

60. Calls on the Council Presidency and the Member States to accelerate their work on the whole Data Protection Package to allow for its adoption in 2014, so that EU citizens will be able to enjoy a high level of data protection in the very near future; stresses that strong engagement and full support on the part of the Council are a necessary condition to demonstrate credibility and assertiveness towards third countries;

61. Stresses that both the Data Protection Regulation and the Data Protection Directive are necessary to protect the fundamental rights of individuals, and that the two must therefore be treated as a package to be adopted simultaneously, in order to ensure that all data-processing activities in the EU provide a high level of protection in all circumstances; stresses that it will only adopt further law enforcement cooperation measures once the Council has entered into negotiations with Parliament and the Commission on the Data Protection Package;

62. Recalls that the concepts of 'privacy by design' and 'privacy by default' are a strengthening of data protection and should have the status of guidelines for all products, services and systems offered on the internet;

63. Considers higher transparency and safety standards for online and telecommunication as a necessary principle with a view to a better data protection regime; calls, therefore, on the Commission to put forward a legislative proposal on standardised general terms and conditions for online and telecommunications services, and to mandate a supervisory body to monitor compliance with the general terms and conditions;

Cloud computing

64. Notes that trust in US cloud computing and cloud providers has been negatively affected by the above-mentioned practices; emphasises, therefore, the development of European clouds and IT solutions as an essential element for growth and employment and for trust in cloud computing services and providers, as well as for ensuring a high level of personal data protection;

65. Calls on all public bodies in the Union not to use cloud services where non-EU laws might apply;

66. Reiterates its serious concern regarding the compulsory direct disclosure of EU personal data and information processed under cloud agreements to third-country authorities by cloud providers subject to third-country laws or using storage servers located in third countries, as also regarding direct remote access to personal data and information processed by third-country law enforcement authorities and intelligence services;

67. Deplores the fact that such access is usually attained by means of direct enforcement by third-country authorities of their own legal rules, without recourse to international instruments established for legal cooperation such as mutual legal assistance (MLA) agreements or other forms of judicial cooperation;

68. Calls on the Commission and the Member States to speed up the work of establishing a European Cloud Partnership while fully including civil society and the technical community, such as the Internet Engineering Task Force (IETF), and incorporating data protection aspects;

69. Urges the Commission, when negotiating international agreements that involve the processing of personal data, to take particular note of the risks and challenges that cloud computing poses to fundamental rights, in particular – but not exclusively – the right to private life and to the protection of personal data, as enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union; urges the Commission, furthermore, to take note of the negotiating partner's domestic rules governing the access of law enforcement and intelligence agencies to personal data processed through cloud computing services, in particular by demanding that such access be granted only if there is full respect for due process of law and on an unambiguous legal basis, as well as the requirement that the exact conditions of access, the purpose of gaining such access, the security measures put in place when handing over data and the rights of the individual, as well as the rules for supervision and for an effective redress mechanism, be specified;

70. Recalls that all companies providing services in the EU must, without exception, comply with EU law and are liable for any breaches, and underlines the importance of having effective, proportionate and dissuasive administrative sanctions in place that can be imposed on 'cloud computing' service providers who do not comply with EU data protection standards;

71. Calls on the Commission and the competent authorities of the Member States to evaluate the extent to which EU rules on privacy and data protection have been violated through the cooperation of EU legal entities with secret services or through the acceptance of court warrants of third-country authorities requesting personal data of EU citizens contrary to EU data protection legislation;

72. Calls on businesses providing new services using 'Big Data' and new applications such as the 'Internet of Things' to build in data protection measures already at the development stage, in order to maintain a high level of trust among citizens;

Transatlantic Trade and Investment Partnership Agreement (TTIP)

73. Recognises that the EU and the US are pursuing negotiations for a Transatlantic Trade and Investment Partnership, which is of major strategic importance for creating further economic growth;

74. Strongly emphasises, given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust, that the consent of the European Parliament to the final TTIP agreement could be endangered as long as the blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not completely abandoned and an adequate solution is found for the data privacy rights of EU citizens, including administrative and judicial redress; stresses that Parliament may only consent to the final TTIP agreement provided the agreement fully respects, inter alia, the fundamental rights recognised by the EU Charter, and provided the protection of the privacy of individuals in relation to the processing and dissemination of personal data remain governed by Article XIV of the GATS; stresses that EU data protection legislation cannot be deemed an 'arbitrary or unjustifiable discrimination' in the application of Article XIV of the GATS;

Democratic oversight of intelligence services

75. Stresses that, despite the fact that oversight of intelligence services' activities should be based on both democratic legitimacy (strong legal framework, ex ante authorisation and ex post verification) and adequate technical capability and expertise, the majority of current EU and US oversight bodies dramatically lack both, in particular the technical capabilities;

76. Calls, as it did in the case of Echelon, on all national parliaments which have not yet done so to install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate; calls on the national parliaments to ensure that such oversight committees/bodies have sufficient resources, technical expertise and legal means, including the right to conduct on-site visits, to be able to effectively control intelligence services;

77. Calls for the setting up of a Group of Members and experts to examine, in a transparent manner and in collaboration with national parliaments, recommendations for enhanced democratic oversight, including parliamentary oversight, of intelligence services and increased oversight collaboration in the EU, in particular as regards its cross-border dimension; considers that the group should examine, in particular, the possibility of minimum European standards or guidelines for the (ex ante and ex post) oversight of intelligence services on the basis of existing best practices and recommendations by international bodies (UN, Council of Europe), including the issue of oversight bodies being considered as a third party under the 'third party rule', or the principle of 'originator control', on the oversight and accountability of intelligence from foreign countries, criteria on enhanced transparency, built on the general principle of access to information and the so-called 'Tshwane Principles'[43], as well as principles regarding the limits on the duration and scope of any surveillance ensuring that they are proportionate and limited to its purpose;

78. Calls on this Group to prepare a report for and to assist in the preparation of a conference to be held by Parliament with national oversight bodies, whether parliamentary or independent, by the beginning of 2015;

79. Calls on the Member States to draw on best practices so as to improve access by their oversight bodies to information on intelligence activities (including classified information and information from other services) and establish the power to conduct on-site visits, a robust set of powers of interrogation, adequate resources and technical expertise, strict independence vis-à-vis their respective governments, and a reporting obligation to their respective parliaments;

80. Calls on the Member States to develop cooperation among oversight bodies, in particular within the European Network of National Intelligence Reviewers (ENNIR);

81. Urges the HR/VP to regularly account for the activities of the EU Intelligence Analysis Centre (IntCen), which is part of the European External Action Service, to the responsible bodies of Parliament, including its full compliance with fundamental rights and applicable EU data privacy rules, allowing for improved oversight by Parliament of the external dimension of EU policies; urges the Commission and the HR/VP to present a proposal for a legal basis for the activities of IntCen, should any operations or future competences in the area of intelligence or data collection facilities of its own be envisaged which may have an impact on the EU's internal security strategy;

---

43 The Global Principles on National Security and the Right to Information, June 2013.

82. Calls on the Commission to present, by December 2014, a proposal for an EU security clearance procedure for all EU office holders, as the current system, which relies on the security clearance undertaken by the Member State of citizenship, provides for different requirements and lengths of procedures within national systems, thus leading to differing treatment of Members of Parliament and their staff depending on their nationality;

83. Recalls the provisions of the interinstitutional agreement between the European Parliament and the Council concerning the forwarding to and handling by Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy, which should be used to improve oversight at EU level;

EU agencies

84. Calls on the Europol Joint Supervisory Body, together with national data protection authorities, to conduct a joint inspection before the end of 2014 in order to ascertain whether information and personal data shared with Europol have been lawfully acquired by national authorities, particularly if the information or data were initially acquired by intelligence services in the EU or a third country, and whether appropriate measures are in place to prevent the use and further dissemination of such information or data; considers that Europol should not process any information or data which were obtained in violation of fundamental rights which would be protected under the Charter of Fundamental Rights;

85. Calls on Europol to make full use of its mandate to request the competent authorities of the Member States to initiate criminal investigations with regards to major cyberattacks and IT breaches with potential cross-border impact; believes that Europol's mandate should be enhanced in order to allow it to initiate its own investigation following suspicion of a malicious attack on the network and information systems of two or more Member States or Union bodies[44]; calls on the Commission to review the activities of Europol's European Cybercrime Centre (EC3) and, if necessary, put forward a proposal for a comprehensive framework for strengthening its competences;

Freedom of expression

86. Expresses its deep concern at the mounting threats to the freedom of the press and the chilling effect on journalists of intimidation by state authorities, in particular as regards the protection of confidentiality of journalistic sources; reiterates the calls expressed in its resolution of 21 May 2013 on 'the EU Charter: standard settings for media freedom across the EU';

87. Takes note of the detention of David Miranda and the seizure of the material in his possession by the UK authorities under Schedule 7 of the Terrorism Act 2000 (and also the request made to the *Guardian* newspaper to destroy or hand over the material) and expresses its concern that this constitutes a possible serious interference with the right of freedom of expression and media freedom as recognised by Article 10 of the ECHR

---

[44] European Parliament position of 25 February 2014 on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) (Texts adopted, P7_TA(2014)0121).

and Article 11 of the EU Charter and that legislation intended to fight terrorism could be misused in such instances;

88. Draws attention to the plight of whistleblowers and their supporters, including journalists following their revelations; calls on the Commission to conduct an examination as to whether a future legislative proposal establishing an effective and comprehensive European whistleblower protection programme, as already requested in Parliament's resolution of 23 October 2013, should also include other fields of Union competence, with particular attention to the complexity of whistleblowing in the field of intelligence; calls on the Member States to thoroughly examine the possibility of granting whistleblowers international protection from prosecution;

89. Calls on the Member States to ensure that their legislation, notably in the field of national security, provides a safe alternative to silence for disclosing or reporting of wrongdoing, including corruption, criminal offences, breaches of legal obligation, miscarriages of justice and abuse of authority, which is also in line with the provisions of different international (UN and Council of Europe) instruments against corruption, the principles laid out in the PACE Resolution 1729 (2010), the Tshwane principles, etc.;

EU IT security

90. Points out that recent incidents clearly demonstrate the acute vulnerability of the EU, and in particular the EU institutions, national governments and parliaments, major European companies, European IT infrastructures and networks, to sophisticated attacks using complex software and malware; notes that these attacks require financial and human resources on a scale such that they are likely to originate from state entities acting on behalf of foreign governments; in this context, regards the case of the hacking or tapping of the telecommunications company Belgacom as a worrying example of an attack on the EU's IT capacity; underlines that boosting EU IT capacity and security also reduces the vulnerability of the EU towards serious cyberattacks originating from large criminal organisations or terrorist groups;

91. Takes the view that the mass surveillance revelations that have initiated this crisis can be used as an opportunity for Europe to take the initiative and build up, as a strategic priority measure, a strong and autonomous IT key-resource capability; stresses that in order to regain trust, such a European IT capability should be based, as much as possible, on open standards and open-source software and if possible hardware, making the whole supply chain from processor design to application layer transparent and reviewable; points out that in order to regain competitiveness in the strategic sector of IT services, a 'digital new deal' is needed, with joint and large-scale efforts by EU institutions, Member States, research institutions, industry and civil society; calls on the Commission and the Member States to use public procurement as leverage to support such resource capability in the EU by making EU security and privacy standards a key requirement in the public procurement of IT goods and services; urges the Commission, therefore, to review the current public procurement practices with regard to data processing in order to consider restricting tender procedures to certified companies, and possibly to EU companies, where security or other vital interests are involved;

92. Strongly condemns the fact that intelligence services sought to lower IT security standards and to install backdoors in a wide range of IT systems; asks the Commission

to present draft legislation to ban the use of backdoors by law enforcement agencies; recommends, consequently, the use of open-source software in all environments where IT security is a concern;

93. Calls on all the Member States, the Commission, the Council and the European Council to give their fullest support, including through funding in the field of research and development, to the development of European innovative and technological capability in IT tools, companies and providers (hardware, software, services and network), including for purposes of cybersecurity and encryption and cryptographic capabilities; calls on all responsible EU institutions and Member States to invest in EU local and independent technologies, and to develop massively and increase detection capabilities;

94. Calls on the Commission, standardisation bodies and ENISA to develop, by December 2014, minimum security and privacy standards and guidelines for IT systems, networks and services, including cloud computing services, in order to better protect EU citizens' personal data and the integrity of all IT systems; believes that such standards could become the benchmark for new global standards and should be set in an open and democratic process, rather than being driven by a single country, entity or multinational company; takes the view that, while legitimate law enforcement and intelligence concerns need to be taken into account in order to support the fight against terrorism, they should not lead to a general undermining of the dependability of all IT systems; expresses support for the recent decisions by the Internet Engineering Task Force (IETF) to include governments in the threat model for internet security;

95. Points out that EU and national telecom regulators, and in certain cases also telecom companies, have clearly neglected the IT security of their users and clients; calls on the Commission to make full use of its existing powers under the ePrivacy and Telecommunication Framework Directive to strengthen the protection of confidentiality of communication by adopting measures to ensure that terminal equipment is compatible with the right of users to control and protect their personal data, and to ensure a high level of security of telecommunication networks and services, including by way of requiring state-of-the-art end-to-end encryption of communications;

96. Supports the EU cyber strategy, but considers that it does not cover all possible threats and should be extended to cover malicious state behaviour; underlines the need for more robust IT security and resilience of IT systems;

97. Calls on the Commission, by January 2015 at the latest, to present an Action Plan to develop greater EU independence in the IT sector, including a more coherent approach to boosting European IT technological capabilities (including IT systems, equipment, services, cloud computing, encryption and anonymisation) and to the protection of critical IT infrastructure (including in terms of ownership and vulnerability);

98. Calls on the Commission, in the framework of the next Work Programme of the Horizon 2020 Programme, to direct more resources towards boosting European research, development, innovation and training in the field of IT, in particular privacy-enhancing technologies and infrastructures, cryptology, secure computing, the best possible security solutions including open-source security, and other information society services, and also to promote the internal market in European software, hardware, and encrypted means of communication and communication infrastructures, including by developing a comprehensive EU industrial strategy for the IT industry; considers that

small and medium enterprises play a particular role in research; stresses that no EU funding should be granted to projects having the sole purpose of developing tools for gaining illegal access into IT systems;

99. Asks the Commission to map out current responsibilities and to review, by December 2014 at the latest, the need for a broader mandate, better coordination and/or additional resources and technical capabilities for ENISA, Europol's Cyber Crime Centre and other Union centres of specialised expertise, CERT-EU and the EDPS, in order to enable them to play a key role in securing European communication systems, be more effective in preventing and investigating major IT breaches in the EU and performing (or assisting Member States and EU bodies to perform) on-site technical investigations regarding major IT breaches; in particular, calls on the Commission to consider strengthening ENISA's role in defending the internal systems within the EU institutions and to establish within ENISA's structure a Computer Emergency Response Team (CERT) for the EU and its Member States;

100. Requests the Commission to assess the need for an EU IT Academy that brings together the best independent European and international experts in all related fields, tasked with providing all relevant EU institutions and bodies with scientific advice on IT technologies, including security-related strategies;

101. Calls on the competent services of the Secretariat of the European Parliament, under the responsibility of the President of Parliament, to carry out, by June 2015 at the latest with an intermediate report by December 2014 at the latest, a thorough review and assessment of Parliament's IT security dependability, focused on: budgetary means, staff resources, technical capabilities, internal organisation and all relevant elements, in order to achieve a high level of security for Parliament's IT systems; believes that such an assessment should at the least provide information, analysis and recommendations on:

- the need for regular, rigorous and independent security audits and penetration tests, with the selection of outside security experts ensuring transparency and guarantees of their credentials vis-à-vis third countries or any types of vested interest;

- the inclusion in tender procedures for new IT systems of best-practice specific IT security/privacy requirements, including the possibility of a requirement for open-source software as a condition of purchase or a requirement that trusted European companies should take part in the tender when sensitive, security-related areas are concerned;

- the list of companies under contract with Parliament in the IT and telecom fields, taking into account any information that has come to light about their cooperation with intelligence agencies (such as revelations about NSA contracts with a company such as RSA, whose products Parliament is using to supposedly protect remote access to their data by its Members and staff), including the feasibility of providing the same services by other, preferably European, companies;

- the reliability and resilience of the software, and especially off-the-shelf commercial software, used by the EU institutions in their IT systems with regard to penetrations and intrusions by EU or third-country law enforcement and intelligence authorities, taking also into account relevant international standards, best-practice security risk

management principles, and adherence to EU Network Information Security standards on security breaches;

– the use of more open-source systems;

– steps and measures to take in order to address the increased use of mobile tools (e.g. smartphones, tablets, whether professional or personal) and its effects on the IT security of the system;

– the security of the communications between the different workplaces of the Parliament and of the IT systems used in Parliament;

– the use and location of servers and IT centres for Parliament's IT systems and the implications for the security and integrity of the systems;

– the implementation in reality of the existing rules on security breaches and prompt notification of the competent authorities by the providers of publicly available telecommunication networks;

– the use of cloud computing and storage services by Parliament, including the nature of the data stored in the cloud, how the content and access to it is protected and where the cloud-servers are located, clarifying the applicable data protection and intelligence legal framework, as well as assessing the possibilities of solely using cloud servers that are based on EU territory;

– a plan allowing for the use of more cryptographic technologies, in particular end-to-end authenticated encryption for all IT and communications services such as cloud computing, email, instant messaging and telephony;

– the use of electronic signatures in email;

– a plan for using a default encryption standard, such as the GNU Privacy Guard, for emails that would at the same time allow for the use of digital signatures;

– the possibility of setting up a secure instant messaging service within Parliament allowing secure communication, with the server only seeing encrypted content;

102. Calls for all the EU institutions and agencies to perform a similar exercise in cooperation with ENISA, Europol and the CERTs, by June 2015 at the latest with an intermediate report by December 2014, in particular the European Council, the Council, the European External Action Service (including EU delegations), the Commission, the Court of Justice and the European Central Bank; invites the Member States to conduct similar assessments;

103. Stresses that as far as the external action of the EU is concerned, assessments of related budgetary needs should be carried out and first measures taken without delay in the case of the European External Action Service (EEAS) and that appropriate funds need to be allocated in the 2015 draft budget;

104. Takes the view that the large-scale IT systems used in the area of freedom, security and justice, such as the Schengen Information System II, the Visa Information System,

Eurodac and possible future systems such as EU-ESTA, should be developed and operated in such a way as to ensure that data are not compromised as a result of requests by authorities from third countries; asks eu-LISA to report back to Parliament on the reliability of the systems in place by the end of 2014;

105. Calls on the Commission and the EEAS to take action at the international level, with the UN in particular, and in cooperation with interested partners to implement an EU strategy for democratic governance of the internet in order to prevent undue influence over ICANN's and IANA's activities by any individual entity, company or country by ensuring appropriate representation of all interested parties in these bodies, while avoiding the facilitation of state control or censorship or the balkanisation and fragmentation of the internet;

106. Calls for the EU to take the lead in reshaping the architecture and governance of the internet in order to address the risks related to data flows and storage, striving for more data minimisation and transparency and less centralised mass storage of raw data, as well as for rerouting of Internet traffic or full end-to-end encryption of all Internet traffic so as to avoid the current risks associated with unnecessary routing of traffic through the territory of countries that do not meet basic standards on fundamental rights, data protection and privacy;

107. Calls for the promotion of:

- EU search engines and EU social networks as a valuable step in the direction of IT independence for the EU;
- European IT service providers;
- encrypting communication in general, including email and SMS communication;
- European IT key elements, for instance solutions for client-server operating systems, using open-source standards, developing European elements for grid coupling, e.g. routers;

108. Calls on the Commission to present a legal proposal for an EU routing system including the processing of call detail records (CDRs) at EU level that will be a substructure of the existing internet and will not extend beyond EU borders; notes that all routing data and CDRs should be processed in accordance with EU legal frameworks;

109. Calls on the Member States, in cooperation with ENISA, Europol's CyberCrime Centre, CERTs and national data protection authorities and cybercrime units, to develop a culture of security and to launch an education and awareness-raising campaign in order to enable citizens to make a more informed choice regarding what personal data to put on-line and how better to protect them, including through encryption and safe cloud computing, making full use of the public interest information platform provided for in the Universal Service Directive;

110. Calls on the Commission, by December 2014, to put forward legislative proposals to encourage software and hardware manufacturers to introduce more security and privacy by design and by default features in their products, including by introducing disincentives for the undue and disproportionate collection of mass personal data and

legal liability on the part of manufacturers for unpatched known vulnerabilities, faulty or insecure products or the installation of secret backdoors enabling unauthorised access to and processing of data; in this respect, calls on the Commission to evaluate the possibility of setting up a certification or validation scheme for IT hardware including testing procedures at EU level to ensure the integrity and security of the products;

Rebuilding trust

111. Believes that, beyond the need for legislative change, the inquiry has shown the need for the US to restore trust with its EU partners, as it is the US intelligence agencies' activities that are primarily at stake;

112. Points out that the crisis of confidence generated extends to:

- the spirit of cooperation within the EU, as some national intelligence activities may jeopardise the attainment of the Union's objectives;

- citizens, who realise that not only third countries or multinational companies but also their own government may be spying on them;

- respect for fundamental rights, democracy and the rule of law, as well as the credibility of democratic, judicial and parliamentary safeguards and oversight in a digital society;

Between the EU and the US

113. Recalls the important historical and strategic partnership between the EU Member States and the US, based on a common belief in democracy, the rule of law and fundamental rights;

114. Believes that the mass surveillance of citizens and the spying on political leaders by the US have caused serious damage to relations between the EU and the US and negatively impacted on trust in US organisations acting in the EU; this is further exacerbated by the lack of judicial and administrative remedies for redress under US law for EU citizens, particularly in cases of surveillance activities for intelligence purposes;

115. Recognises, in light of the global challenges facing the EU and the US, that the transatlantic partnership needs to be further strengthened, and that it is vital that transatlantic cooperation in counter-terrorism continues on a new basis of trust based on true common respect for the rule of law and the rejection of all indiscriminate practices of mass surveillance; insists, therefore, that clear measures need to be taken by the US to re-establish trust and re-emphasise the shared basic values underlying the partnership;

116. Is ready to engage in a dialogue with US counterparts so that, in the ongoing American public and congressional debate on reforming surveillance and reviewing intelligence oversight, the right to privacy and other rights of EU citizens, residents or other persons protected by EU law and equivalent information rights and privacy protection in US courts, including legal redress, are guaranteed through, for example, a revision of the Privacy Act and the Electronic Communications Privacy Act and by ratifying the First Optional Protocol to the International Covenant on Civil and Political Rights (ICCPR), so that the current discrimination is not perpetuated;

117. Insists that necessary reforms be undertaken and effective guarantees be given to Europeans to ensure that the use of surveillance and data processing for foreign intelligence purposes is proportional, limited by clearly specified conditions, and related to reasonable suspicion and probable cause of terrorist activity; stresses that this purpose must be subject to transparent judicial oversight;

118. Considers that clear political signals are needed from our American partners to demonstrate that the US distinguishes between allies and adversaries;

119. Urges the Commission and the US Administration to address, in the context of the ongoing negotiations on an EU-US Umbrella Agreement on data transfer for law enforcement purposes, the information and judicial redress rights of EU citizens, and to conclude these negotiations, in line with the commitment made at the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013, before summer 2014;

120. Encourages the US to accede to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as it acceded to the 2001 Convention on Cybercrime, thus strengthening the shared legal basis between the transatlantic allies;

121. Calls on the EU institutions to explore the possibilities for establishing with the US a code of conduct which would guarantee that no US espionage is pursued against EU institutions and facilities;

Within the European Union

122. Also believes that the involvement and activities of EU Member States have led to a loss of trust, including among Member States and between EU citizens and their national authorities; is of the opinion that only full clarity as to purposes and means of surveillance, public debate and, ultimately, revision of legislation, including an end to mass surveillance activities and strengthening the system of judicial and parliamentary oversight, will it be possible to re-establish the trust lost; reiterates the difficulties involved in developing comprehensive EU security policies with such mass surveillance activities in operation, and stresses that the EU principle of sincere cooperation requires that Member States refrain from conducting intelligence activities in other Member States' territory;

123. Notes that some Member States are pursuing bilateral communication with the US authorities on spying allegations, and that some of them have concluded (the UK) or envisage concluding (Germany, France) so-called 'anti-spying' arrangements; stresses that these Member States need to observe fully the interests and the legislative framework of the EU as a whole; deems such bilateral arrangements to be counterproductive and irrelevant, given the need for a European approach to this problem; asks the Council to inform Parliament on developments by Member States on an EU-wide mutual no-spy arrangement;

124. Considers that such arrangements should not breach the Union Treaties, especially the principle of sincere cooperation (under Article 4(3) TEU), or undermine EU policies in general and, more specifically, the internal market, fair competition, and economic, industrial and social development; decides to review any such arrangements for their compatibility with European law, and reserves the right to activate Treaty procedures in

the event of such arrangements being proven to contradict the Union's cohesion or the fundamental principles on which it is based;

125. Calls on the Member States to make every effort to ensure better cooperation with a view to providing safeguards against espionage, in cooperation with the relevant EU bodies and agencies, for the protection of EU citizens and institutions, European companies, EU industry, and IT infrastructure and networks, as well as European research; considers the active involvement of EU stakeholders to be a precondition for an effective exchange of information; points out that security threats have become more international, diffuse and complex, thereby requiring an enhanced European cooperation; believes that this development should be better reflected in the Treaties, and therefore calls for a revision of the Treaties in order to reinforce the notion of sincere cooperation between the Member States and the Union as regards the objective of achieving an area of security and to prevent mutual espionage between Member States within the Union;

126. Considers tap-proof communication structures (email and telecommunications, including landlines and cell phones) and tap-proof meeting rooms within all relevant EU institutions and EU delegations to be absolutely necessary; therefore calls for the establishment of an encrypted internal EU email system;

127. Calls on the Council and Commission to consent without further delay to the proposal adopted by the European Parliament on 23 May 2012 for a regulation of the European Parliament on the detailed provisions governing the exercise of the European Parliament's right of inquiry and repealing Decision 95/167/EC, Euratom, ECSC of the European Parliament, the Council and the Commission presented on the basis of Article 226 TFEU; calls for a revision of the Treaty in order to extend such inquiry powers to cover, without restrictions or exceptions, all fields of Union competence or activity and to include the possibility of questioning under oath;

Internationally

128. Calls on the Commission to present, by January 2015 at the latest, an EU strategy for democratic governance of the internet;

129. Calls on the Member States to follow the call of the 35th International Conference of Data Protection and Privacy Commissioners ‘to advocate the adoption of an additional protocol to Article17 of the International Covenant on Civil and Political Rights (ICCPR), which should be based on the standards that have been developed and endorsed by the International Conference and the provisions in the Human Rights Committee General Comment No 16 to the Covenant in order to create globally applicable standards for data protection and the protection of privacy in accordance with the rule of law’; calls on the Member States to include in this exercise a call for an international UN agency to be in charge of, in particular, monitoring the emergence of surveillance tools and regulating and investigating their uses; asks the High Representative/Vice-President of the Commission and the European External Action Service to take a proactive stance;

130. Calls on the Member States to develop a coherent and strong strategy within the UN, supporting in particular the resolution on ‘the right to privacy in the digital age’ initiated by Brazil and Germany, as adopted by the Third Committee of the UN General

Assembly Committee (Human Rights Committee) on 27 November 2013, as well as taking further action for the defence of the fundamental right to privacy and data protection at an international level while avoiding any facilitation of state control or censorship or the fragmentation of the internet, including an initiative for an international treaty prohibiting mass surveillance activities and an agency for its oversight;

Priority Plan: A European Digital Habeas Corpus - protecting fundamental rights in a digital age

131. Decides to submit to EU citizens, institutions and Member States the above-mentioned recommendations as a Priority Plan for the next legislature; calls on the Commission and the other EU institutions, bodies, offices and agencies referred to in this resolution, in accordance with Article 265 TFEU, to act upon the recommendations and calls as contained in this resolution;

132. Decides to launch 'A European Digital Habeas Corpus - protecting fundamental rights in a digital age' with the following 8 actions, the implementation of which it will oversee:

- Action 1: Adopt the Data Protection Package in 2014;

- Action 2: Conclude the EU-US Umbrella Agreement guaranteeing the fundamental right of citizens to privacy and data protection and ensuring proper redress mechanisms for EU citizens, including in the event of data transfers from the EU to the US for law enforcement purposes;

- Action 3: Suspend Safe Harbour until a full review has been conducted and current loopholes are remedied, making sure that transfers of personal data for commercial purposes from the Union to the US can only take place in compliance with the highest EU standards;

- Action 4: Suspend the TFTP agreement until: (i) the Umbrella Agreement negotiations have been concluded; (ii) a thorough investigation has been concluded on the basis of an EU analysis and all concerns raised by Parliament in its resolution of 23 October 2013 have been properly addressed;

- Action 5: Evaluate any agreement, mechanism or exchange with third countries involving personal data in order to ensure that the right to privacy and to the protection of personal data is not violated due to surveillance activities, and take necessary follow-up actions;

- Action 6: Protect the rule of law and the fundamental rights of EU citizens, (including from threats to the freedom of the press), the right of the public to receive impartial information and professional confidentiality (including lawyer-client relations), as well as ensuring enhanced protection for whistleblowers;

- Action 7: Develop a European strategy for greater IT independence (a 'digital new deal' including the allocation of adequate resources at national and EU level) in order to boost IT industry and allow European companies to exploit the EU privacy competitive advantage;

– Action 8: Develop the EU as a reference player for a democratic and neutral governance of the internet;

133. Calls on the EU institutions and the Member States to promote the 'European Digital Habeas Corpus' protecting fundamental rights in a digital age; undertakes to act as the EU citizens' rights advocate, with the following timetable to monitor implementation:

– April 2014-March 2015: a monitoring group based on the LIBE inquiry team responsible for monitoring any new revelations concerning the inquiry's mandate and scrutinising the implementation of this resolution;

– July 2014 onwards: a standing oversight mechanism for data transfers and judicial remedies within the competent committee;

– Spring 2014: a formal call on the European Council to include the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' in the guidelines to be adopted under Article 68 TFEU;

– Autumn 2014: a commitment that the 'European Digital Habeas Corpus - protecting fundamental rights in a digital age' and related recommendations will serve as key criteria for the approval of the next Commission;

– 2014: a conference bringing together high-level European experts in the various fields conducive to IT security (including mathematics, cryptography and privacy-enhancing technologies) to help foster an EU IT strategy for the next legislative term;

– 2014-2015: a Trust/Data/Citizens' Rights group to be convened on a regular basis between the European Parliament and the US Congress, as well as with other committed third-country parliaments, including that of Brazil;

– 2014-2015: a conference with the intelligence oversight bodies of European national parliaments;

o

o o

134. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the parliaments and governments of the Member States, the national data protection authorities, the EDPS, eu-LISA, ENISA, the Fundamental Rights Agency, the Article 29 Working Party, the Council of Europe, the Congress of the United States of America, the US Administration, the President, Government and Parliament of the Federative Republic of Brazil, and the UN Secretary-General;

135. Instructs its Committee on Civil Liberties, Justice and Home Affairs to address Parliament in plenary on the matter a year after the adoption of this resolution; considers it essential to assess the extent to which the recommendations adopted by Parliament have been followed and to analyse any instances where such recommendations have not been followed;

P7_TA-PROV(2014)0230

Programme de surveillance de la NSA, organismes de surveillance dans divers États membres et incidences sur les droits fondamentaux des citoyens européens

Résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI))

Le Parlement européen,

– vu le traité sur l'Union européenne (traité UE), et notamment ses articles 2, 3, 4, 5, 6, 7, 10, 11 et 21,

– vu le traité sur le fonctionnement de l'Union européenne (traité FUE) et, en particulier, ses articles 15, 16 et 218 et son titre V,

– vu le protocole n° 36 sur les dispositions transitoires, notamment son article 10, ainsi que la déclaration 50 relative à ce protocole,

– vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 1, 3, 6, 7, 8, 10, 11, 20, 21, 42, 47, 48 et 52,

– vu la convention européenne des droits de l'homme (CEDH), et notamment ses articles 6, 8, 9, 10 et 13, ainsi que ses protocoles annexes,

– vu la déclaration universelle des droits de l'homme, et notamment ses articles 7, 8, 10, 11, 12 et 14[45],

– vu le pacte international relatif aux droits civils et politiques, notamment ses articles 14, 17, 18 et 19,

– vu la convention du Conseil de l'Europe pour la protection des données (STE n° 108) et le protocole additionnel du 8 novembre 2001 à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181),

– vu la convention de Vienne sur les relations diplomatiques, en particulier ses articles 24, 27 et 40,

– vu la convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185),

---

[45] http://www.un.org/fr/documents/udhr/.

– vu le rapport du rapporteur spécial des Nations unies pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme, remis le 17 mai 2010[46],

– vu la communication de la Commission intitulée "Politique et gouvernance de l'internet : le rôle de l'Europe à l'avenir" (COM(2014)0072),

– vu le rapport du rapporteur spécial des Nations unies sur la promotion et la protection de la liberté d'opinion et d'expression, remis le 17 avril 2013[47],

– vu les lignes directrices sur les droits de l'homme et la lutte contre le terrorisme adoptées par le Comité des ministres du Conseil de l'Europe en date du 11 juillet 2002,

– vu la déclaration de Bruxelles du 1er octobre 2010, adoptée lors de la 6e conférence des commissions parlementaires de contrôle des services de renseignements et de sécurité des États membres de l'Union européenne,

– vu la résolution 1954(2013) de l'Assemblée parlementaire du Conseil de l'Europe sur la sécurité nationale et l'accès à l'information,

– vu le rapport sur le contrôle démocratique des services de sécurité adopté par la Commission de Venise le 11 juin 2007[48], dont il attend avec grand intérêt la mise à jour, prévue au printemps 2014,

– vu les témoignages des représentants des commissions de contrôle des services de renseignement de Belgique, des Pays-Bas, du Danemark et de Norvège,

– vu les affaires introduites auprès des tribunaux français[49], polonais et britanniques[50], ainsi qu'auprès de la Cour européenne des droits de l'homme[51], en ce qui concerne les systèmes de surveillance de masse,

– vu la convention établie par le Conseil conformément à l'article 34 du traité sur l'Union européenne, relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[52], et en particulier son titre III,

---

46 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement

47 http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

48 http://www.venice.coe.int/webforms/documents/default.aspx?ref=cdl-ad(2007)016&lang=fr.

49 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.

50 Affaires introduites par Privacy International and Liberty auprès de l'Investigatory Powers Tribunal.

51 Requête conjointe au titre de l'article 34 introduite par Big Brother Watch, Open Rights Group, English Pen, Dr Constanze Kurz (parties demanderesses) contre le Royaume-Uni (partie défenderesse).

52 JO C 197 du 12.7.2000, p. 1.

– vu la décision 2000/520/CE de la Commission, du 26 juillet 2000, relative à la pertinence de la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique,

– vu les rapports d'évaluation de la Commission sur l'application des principes de la "sphère de sécurité" du 13 février 2002 (SEC(2002)0196) et du 20 octobre 2004 (SEC(2004)1323),

– vu la communication de la Commission du 27 novembre 2013 sur le fonctionnement de la "sphère de sécurité" du point de vue des citoyens européens et des entreprises établies dans l'Union (COM(2013)0847) et la communication de la Commission du 27 novembre 2013 sur le rétablissement de la confiance à l'égard des flux de données entre l'Union européenne et les États-Unis (COM(2013)0846),

– vu sa résolution du 5 juillet 2000 sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la "sphère de sécurité" et les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis[53], qui a estimé que la pertinence du système ne pouvait être confirmée, ainsi que les avis du groupe de travail "Article 29", en particulier l'avis 4/2000 du 16 mai 2000[54],

– vu les accords conclus entre les États-Unis d'Amérique et l'Union européenne en 2004, 2007[55] et 2012[56] sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure,

– vu l'examen conjoint de la mise en œuvre de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert des données des dossiers passagers au ministère américain de la sécurité intérieure[57] accompagnant le rapport de la Commission au Parlement européen et au Conseil sur l'examen conjoint (COM(2013)0844),

– vu l'avis de l'avocat général Cruz Villalón concluant que la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications est globalement incompatible avec l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne et que son article 6 est incompatible avec les articles 7 et 52, paragraphe 1, de la charte[58];

– vu la décision 2010/412/UE du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux

---

53 JO C 121 du 24.4.2001, p. 152.
54 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp32fr.pdf.
55 JO L 204 du 4.8.2007, p. 18.
56 JO L 215 du 11.8.2012, p. 5.
57 SEC(2013)0630 du 27.11.2013.
58 Avis de l'avocat général Cruz Villalón du 12 décembre 2013 dans l'affaire C-293/12.

fins du programme de surveillance du financement du terrorisme (TFTP)[59], ainsi que les déclarations de la Commission et du Conseil qui l'accompagnaient,

– vu l'accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire[60],

– vu les négociations en cours sur un accord-cadre entre l'Union européenne et les États-Unis d'Amérique relatif à la protection des données à caractère personnel lors de leur transfert et de leur traitement aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et judiciaire en matière pénale ("l'accord-cadre"),

– vu le règlement (CE) n° 2271/96 du Conseil du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant[61],

– vu la déclaration de la présidente de la République fédérale du Brésil lors de l'ouverture de la 68e session de l'Assemblée générale des Nations unies le 24 septembre 2013 et les travaux réalisés par la commission parlementaire d'enquête sur l'espionnage créée par le Sénat fédéral du Brésil,

– vu le Patriot Act des États-Unis, signé par le président George W. Bush le 26 octobre 2001,

– vu la loi de 1978 sur la surveillance et le renseignement étranger (FISA) et la loi de 2008 portant modification de la FISA,

– vu le décret exécutif n° 12333 adopté par le président américain en 1981 et modifié en 2008,

– vu la directive présidentielle n° 28 (Presidential Policy Directive – PPD-28) sur le renseignement d'origine électromagnétique promulguée par Barack Obama, président des États-Unis, le 17 janvier 2014,

– vu les propositions législatives en cours d'examen par le Congrès américain, dont le projet de loi sur la liberté (US Freedom Act) ou le projet de loi sur le contrôle du renseignement et la réforme de la surveillance, entre autres,

– vu les études réalisées par le Conseil de surveillance de la vie privée et des libertés civiles, le Conseil de sécurité nationale des États-Unis et le groupe d'étude du président sur la révision des renseignements et des technologies, en particulier le rapport publié par ce dernier le 12 décembre 2013 et intitulé "Liberty and Security in a Changing World",

– vu la décision du tribunal de district des États-Unis pour le district de Columbia, Klayman e.a. /Obama e.a., action civile n° 13-0851 du 16 décembre 2013, ainsi que la décision du tribunal de district des États-Unis pour le district sud de New York, ACLU e.a. / James R. Clapper e.a, action civile n° 13-3994 du 11 juin 2013,

---

59 JO L 195 du 27.7.2010, p. 3.
60 JO L 181 du 19.7.2003, p. 34.
61 JO L 309 du 29.11.1996, p. 1.

– vu le rapport sur les conclusions des coprésidents de l'Union européenne du groupe de travail UE-États-Unis sur la protection des données du 27 novembre 2013[62],

– vu ses résolutions du 5 septembre 2001[63] et du 7 novembre 2002[64] sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON),

– vu sa résolution du 21 mai 2013 sur la charte de l'UE: ensemble de normes pour la liberté des médias à travers l'UE[65],

– vu sa résolution du 4 juillet 2013 sur le programme de surveillance de l'agence nationale de sécurité américaine (NSA), les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union[66], dans laquelle il chargeait sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur cette question,

– vu le document de travail n°1 sur les programmes de surveillance des États-Unis et de l'Union européenne et leur impact sur les droits fondamentaux des citoyens de l'Union,

– vu le document de travail n° 3 sur la relation entre les pratiques de surveillance dans l'Union et les dispositions de l'Union européenne et des États-Unis en matière de protection des données,

– vu le document de travail n° 4 relatif aux activités de surveillance des États-Unis à l'égard des données de l'Union européenne et à leurs implications juridiques éventuelles sur les accords et la coopération transatlantiques,

– vu le document de travail n° 5 sur le contrôle démocratique des services de renseignement des États membres et des organes de renseignement de l'Union européenne,

– vu le document de travail de la commission des affaires étrangères sur les aspects de politique étrangère de l'enquête sur la surveillance électronique de masse des citoyens de l'Union européenne;

– vu sa résolution du 23 octobre 2013 sur la criminalité organisée, la corruption et le blanchiment de capitaux: recommandations sur des actions et des initiatives à entreprendre[67],

– vu sa résolution du 23 octobre 2013 sur la suspension de l'accord TFTP du fait de la surveillance exercée par l'agence nationale de sécurité américaine[68],

– vu sa résolution du 10 décembre 2013 sur l'exploitation du potentiel de l'informatique en nuage en Europe[69],

---

62 Document du Conseil 16987/2013.

63 JO C 72 E du 21.3.2002, p. 221.

64 JO C 16 E du 22.1.2004, p. 88.

65 Textes adoptés de cette date, P7_TA(2013)0203.

66 Textes adoptés de cette date, P7_TA(2013)0322.

67 Textes adoptés de cette date, P7_TA(2013)0444.

68 Textes adoptés de cette date, P7_TA(2013)0449.

– vu l'accord interinstitutionnel entre le Parlement européen et le Conseil relatif à la transmission au Parlement européen et au traitement par celui-ci des informations classifiées détenues par le Conseil concernant des questions autres que celles relevant de la politique étrangère et de sécurité commune[70],

– vu l'annexe VIII de son règlement,

– vu l'article 48 de son règlement,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A7-0139/2014),

Les incidences de la surveillance de masse

A. considérant que la protection des données et la vie privée sont des droits fondamentaux; considérant que les mesures de sécurité, notamment dans le cadre de la lutte contre le terrorisme, doivent donc s'inscrire dans l'état de droit et respecter les obligations en matière de droits de l'homme, y compris celles qui ont trait à la vie privée et à la protection des données;

B. considérant que les flux d'information et les données, qui dominent aujourd'hui la vie quotidienne et font partie de l'intégrité de toute personne, doivent être aussi sûrs que les domiciles devant les intrusions;

C. considérant que les liens entre l'Europe et les États-Unis d'Amérique sont fondés sur l'esprit et les principes de démocratie et d'état de droit, de liberté, de justice et de solidarité;

D. considérant que la coopération entre les États-Unis et l'Union européenne et ses États membres dans le domaine de la lutte contre le terrorisme restent d'une importance cruciale pour la sécurité et la sûreté des deux partenaires;

E. considérant que la confiance et la compréhension mutuelles constituent des facteurs clés dans le dialogue et le partenariat transatlantiques;

F. considérant qu'après le 11 septembre 2001, la lutte contre le terrorisme est devenue l'une des grandes priorités de la plupart des gouvernements; considérant que les révélations fondées sur les documents divulgués par Edward Snowden, ancien consultant de la NSA, ont contraint les dirigeants politiques à faire face aux défis de la supervision et du contrôle des agences de renseignement dans le cadre de leurs activités de surveillance et à évaluer les incidences de leurs activités sur les droits fondamentaux et l'état de droit dans la société démocratique;

G. considérant que les révélations faites depuis juin 2013 ont suscité de nombreuses inquiétudes au sein de l'Union en ce qui concerne:

  – la portée des systèmes de surveillance révélée aux États-Unis et dans les États membres de l'Union;

---

[69] Textes adoptés de cette date, P7_TA(2013)0535.

[70] JO C 353 E du 3.12.2013, p. 156.

– la violation des normes juridiques et des droits fondamentaux de l'Union européenne ainsi que des normes européennes en matière de protection des données;

– le niveau de confiance entre les partenaires transatlantiques que sont l'Union européenne et les États-Unis;

– le degré de coopération et d'implication de certains États membres de l'Union dans des programmes de surveillance américains ou programmes équivalents au niveau national, comme l'ont révélé les médias;

– le manque de contrôle et de surveillance effective par les autorités politiques américaines et certains États membres de l'Union européenne sur leurs services de renseignement;

– la possibilité que ces activités de surveillance de masse soient utilisées pour des raisons autres que la sécurité nationale et la lutte contre le terrorisme au sens strict, par exemple à des fins d'espionnage économique et industriel ou de profilage pour des motifs politiques;

– l'atteinte à la liberté de la presse et aux communications des membres des professions soumises au secret professionnel, dont les avocats et les médecins;

– les rôles et degrés d'implication respectifs des agences de renseignement et des entreprises informatiques et de télécommunications privées;

– les frontières de plus en plus floues entre les activités répressives et les activités de renseignement, avec pour effet que chaque citoyen est traité comme un suspect et fait l'objet d'une surveillance;

– les menaces relatives à la vie privée à l'heure du numérique et l'incidence de la surveillance de masse sur les citoyens et les sociétés;

H. considérant que l'ampleur sans précédent des activités d'espionnage révélées nécessite une enquête approfondie de la part des autorités américaines, des institutions européennes, et des gouvernements et des parlements nationaux des États membres ainsi que de leurs autorités judiciaires;

I. considérant que les autorités américaines ont réfuté certaines des informations divulguées, mais n'ont pas contesté la grande majorité de celles-ci; que le débat public a pris une grande ampleur aux États-Unis ainsi que dans certains États membres de l'Union européenne; que les gouvernements et les parlements européens restent encore trop souvent silencieux et ne lancent pas d'enquêtes adéquates;

J. considérant que M. Obama a récemment annoncé une réforme de la NSA et de ses programmes de surveillance;

K. considérant qu'en comparaison des mesures prises par les institutions européennes et par certains États membres, le Parlement européen a pris très au sérieux son obligation de faire la lumière sur les révélations des pratiques non sélectives de surveillance de masse des citoyens européens et, par sa résolution du 4 juillet 2013 sur le programme de

surveillance de l'agence nationale de sécurité américaine, les organismes de surveillance de plusieurs États membres et leur impact sur la vie privée des citoyens de l'Union, a chargé sa commission des libertés civiles, de la justice et des affaires intérieures de mener une enquête approfondie sur la question;

L. considérant qu'il est du devoir des institutions européennes de veiller à ce que le droit de l'Union soit pleinement mis en œuvre dans l'intérêt des citoyens européens et que la force juridique des traités de l'Union ne soit pas compromise par un mépris des effets extraterritoriaux des normes ou actions des pays tiers;

Évolution de la réforme des services de renseignement aux États-Unis

M. considérant que le tribunal de district des États-Unis pour le district de Columbia a jugé, dans sa décision du 16 décembre 2013, que la collecte massive de métadonnées par la NSA contrevenait au quatrième amendement à la constitution des États-Unis[71]; qu'en revanche, le tribunal de district pour le district sud de New York a jugé que cette collecte était légale dans sa décision du 27 décembre 2013;

N. considérant qu'une décision du tribunal de district de la région orientale de l'État du Michigan a considéré que le quatrième amendement exigeait l'existence d'un caractère raisonnable pour toutes les recherches effectuées, des mandats préalables pour toutes les recherches raisonnables, des mandats basés sur une cause probable préexistante, ainsi qu'une prise en considération des particularités des personnes, des endroits et des objets et l'interposition d'un magistrat neutre entre les agents répressifs du pouvoir exécutif et les citoyens[72];

O. considérant que dans son rapport du 12 décembre 2013, le groupe d'étude du président sur la révision des renseignements et des technologies propose 46 recommandations au président des États-Unis; que ces recommandations soulignent la nécessité de protéger à la fois la sécurité nationale et la vie privée et les libertés civiles; qu'il invite, à cet égard, le gouvernement américain: à mettre fin dans les plus brefs délais à la collecte massive d'enregistrements téléphoniques de citoyens américains au titre de la section 215 du Patriot Act; à entreprendre un examen approfondi de la NSA et du cadre juridique américain en matière de renseignement afin de garantir le respect du droit à la vie privée; à cesser les efforts visant à saboter ou rendre vulnérables les logiciels commerciaux (chevaux de Troie et logiciels malveillants); à accroître l'utilisation du cryptage, particulièrement en ce qui concerne les données en transit, et à ne pas saper les efforts visant à créer des normes de cryptage; à nommer un représentant de l'intérêt public chargé de défendre la vie privée et les libertés civiles devant la cour dite FISC (Foreign Intelligence Surveillance Court); à conférer au Conseil de surveillance de la vie privée et des libertés civiles le pouvoir de superviser les activités des services de renseignement à des fins de renseignement étranger, et pas uniquement à des fins de lutte contre le terrorisme; et à recevoir les plaintes de lanceurs d'alerte, à utiliser les traités en matière d'entraîne judiciaire pour obtenir des communications électroniques et à ne pas utiliser la surveillance pour voler des secrets industriels ou commerciaux;

P. considérant que, selon un mémorandum public remis à M. Obama par les anciens hauts responsables de la NSA (Veteran Intelligence Professionals for Sanity) le 7 janvier

---

[71] Klayman e.a./Obama e.a.., action civile n° 13-0851, 16 décembre 2013.

[72] ACLU/ NSA n° 06-CV-10204, 17 août 2006.

2014[73], la collecte massive de données ne renforce pas la capacité de la NSA à prévenir de futures attaques terroristes; que les auteurs soulignent que la surveillance de masse réalisée par la NSA n'a prévenu aucune attaque et que des milliards de dollars ont été dépensés dans des programmes moins efficaces et considérablement plus irrespectueux de la vie privée des citoyens qu'une technologie baptisée THINTHREAD développée en interne en 2001;

Q. considérant qu'en ce qui concerne les activités de renseignement relatives à des ressortissants non américains au sens de la section 702 de la FISA, les recommandations adressées au président des États-Unis reconnaissent le principe fondamental du respect de la vie privée et de la dignité humaine consacré à l'article 12 de la déclaration universelle des droits de l'homme et à l'article 17 du pacte international relatif aux droits civils et politiques; que ces recommandations ne préconisent pas d'octroyer aux ressortissants non américains les mêmes droits et protections qu'aux ressortissants américains;

R. considérant que, dans sa directive présidentielle sur le renseignement électromagnétique (Presidential Policy Directive on Signals Intelligence Activties) du 17 janvier 2014 et le discours associé, le président Barack Obama a déclaré que la surveillance électronique de masse était nécessaire pour permettre aux États-Unis d'assurer la sécurité nationale, de protéger leurs citoyens et les citoyens de leurs alliés et partenaires, ainsi que de promouvoir leurs intérêts en matière de politique étrangère; considérant que cette directive comporte certains principes relatifs au recueil, à l'utilisation et au partage des renseignements électromagnétiques et étend certaines garanties à des citoyens non américains, en accordant en partie un traitement équivalent à celui dont bénéficient les ressortissants américains, dont des garanties concernant les informations personnelles de tous, indépendamment de la nationalité ou du lieu de résidence; considérant cependant que le président Obama n'a préconisé aucune proposition concrète, en particulier en ce qui concerne l'interdiction des activités de surveillance de masse et l'instauration de voies de recours administratives et juridictionnelles pour les ressortissants non américains;

Cadre juridique

Droits fondamentaux

S. considérant que le rapport sur les conclusions des coprésidents de l'Union du groupe de travail ad hoc UE-États-Unis sur la protection des données donne un aperçu de la situation juridique aux États-Unis, mais n'a pas permis d'établir les faits relatifs aux programmes de surveillance américains; qu'aucune information n'a été donnée au sujet du groupe de travail dit de "deuxième voie", dans le cadre duquel les États membres discutent bilatéralement avec les autorités américaines des questions ayant trait à la sécurité nationale;

T. considérant que les droits fondamentaux, notamment les libertés d'expression, de la presse, de pensée, de conscience, de religion et d'association, le respect de la vie privée, la protection des données, ainsi que le droit à un recours effectif, la présomption d'innocence et le droit à un procès équitable et à la non-discrimination, consacrés dans la charte des droits fondamentaux de l'Union européenne et la convention européenne

[73] http://consortiumnews.com/2014/01/07/nsa-insiders-reveal-what-went-wrong.

des droits de l'homme, constituent des pierres angulaires de la démocratie; considérant que la surveillance de masse des êtres humains est incompatible avec celles-ci;

U. considérant que dans tous les États membres, le droit protège contre la divulgation d'informations communiquées à titre confidentiel entre un avocat et son client, principe reconnu par la Cour de justice de l'Union européenne[74];

V. considérant que dans sa résolution du 23 octobre 2013 sur la criminalité organisée, la corruption et le blanchiment de capitaux, il invite la Commission à présenter une proposition législative visant à mettre en place un programme européen efficace et complet de protection des lanceurs d'alerte afin de protéger les intérêts financiers de l'Union européenne et à examiner s'il convient d'étendre ces futures dispositions à d'autres domaines de compétence de l'Union;

Compétences de l'Union dans le domaine de la sécurité

W. considérant qu'en vertu de l'article 67, paragraphe 3, du traité FUE, l'Union européenne "œuvre pour assurer un niveau élevé de sécurité"; que les dispositions du traité (notamment l'article 4, paragraphe 2, du traité UE, ainsi que les articles 72 et 73 du traité FUE) signifient que l'Union européenne est dotée de certaines compétences sur les questions ayant trait à la sécurité collective de l'Union; que l'Union est compétente dans les domaines relatifs à la sécurité intérieure (article 4, paragraphe 2, point j), du traité FUE) et exerce cette compétence en adoptant un certain nombre d'instruments législatifs et en concluant des accords internationaux (sur les données PNR, le TFTP) visant à lutter contre la grande criminalité et le terrorisme ainsi qu'en élaborant une stratégie pour la sécurité intérieure et des agences travaillant dans ce domaine;

X. considérant que le traité sur le fonctionnement de l'Union européenne dispose qu'"il est loisible aux États membres d'organiser entre eux et sous leur responsabilité des formes de coopération et de coordination qu'ils jugent appropriées entre les services compétents de leurs administrations chargées d'assurer la sécurité nationale" (article 73 du traité FUE);

Y. considérant que l'article 276 du traité sur le fonctionnement de l'Union européenne dispose que "dans l'exercice de ses attributions concernant les dispositions des chapitres 4 et 5 du titre V, de la troisième partie, relatives à l'espace de liberté, de sécurité et de justice, la Cour de justice de l'Union européenne n'est pas compétente pour vérifier la validité ou la proportionnalité d'opérations menées par la police ou d'autres services répressifs dans un État membre, ni pour statuer sur l'exercice des responsabilités qui incombent aux États membres pour le maintien de l'ordre public et la sauvegarde de la sécurité intérieure";

Z. considérant que les notions de "sécurité nationale", de "sécurité intérieure", de "sécurité intérieure de l'Union" et de "sécurité internationale" se recoupent; que la convention de Vienne sur le droit des traités, le principe de coopération loyale entre États membres de l'Union et le principe du droit international humanitaire consistant à interpréter étroitement toute dérogation suggèrent une interprétation restrictive de la notion de

---

[74] Arrêt du 18 mai 1982 dans l'affaire C-155/79, AM & S Europe Limited / Commission des Communautés européennes.

"sécurité nationale" et exigent que les États membres s'abstiennent d'empiéter sur les compétences de l'Union;

AA. considérant que les traités européens assignent à la Commission le rôle de "gardienne des traités" et donc, que la Commission est légalement tenue d'enquêter sur toute violation éventuelle du droit de l'Union;

AB. considérant que, conformément à l'article 6 du traité sur l'Union européenne, où il est fait référence à la charte des droits fondamentaux de l'Union européenne et à la CEDH, les agences des États membres et même les parties privées agissant dans le domaine de la sécurité nationale sont aussi tenues de respecter les droits consacrés par les dispositions de ces deux textes, tant à l'égard de leurs propres citoyens ou que des citoyens des autres États;

Extraterritorialité

AC. considérant que l'application extraterritoriale, par un pays tiers, de ses lois, règlements et autres instruments législatifs ou exécutifs dans des situations relevant de la compétence de l'Union européenne ou de ses États membres peut avoir des répercussions sur l'ordre juridique établi et l'état de droit, voire violer le droit international ou européen, notamment les droits de personnes physiques et morales, en tenant compte de l'étendue et de l'objectif officiel ou officieux d'une telle application; que, dans ces circonstances, il est nécessaire d'entreprendre une action au niveau de l'Union afin de garantir le respect sur son territoire des valeurs de l'Union consacrées par l'article 2 du traité UE, par la charte des droits fondamentaux et par la CEDH concernant les droits fondamentaux, la démocratie et l'état de droit, et des droits des personnes physiques ou morales consacrés dans la législation dérivée appliquant ces principes fondamentaux, notamment en éliminant, en neutralisant, en bloquant ou en contrecarrant de toute autre manière les effets de la législation étrangère en cause;

Transferts internationaux de données

AD. considérant que le transfert de données à caractère personnel par les institutions, organes ou organismes de l'Union ou par les États membres vers les États-Unis à des fins répressives en l'absence de garanties et de protections adéquates concernant le respect des droits fondamentaux des citoyens de l'Union, notamment les droits à la vie privée et à la protection des données à caractère personnel, engagerait la responsabilité de l'institution, organe ou organisme ou l'État membre en question, au titre de l'article 340 du traité FUE ou de la jurisprudence constante de la CJUE[75] pour violation du droit de l'Union – y compris toute violation des droits fondamentaux consacrés dans la charte de l'Union européenne;

AE. considérant que le transfert de données n'est pas limité sur le plan géographique et que, notamment eu égard au développement de la mondialisation et des communications à l'échelle mondiale, le législateur européen fait face à de nouveaux défis en matière de protection des données et des communications à caractère personnel; qu'il est donc de la plus grande importance de promouvoir les cadres juridiques établissant des règles communes;

---

[75] Voir notamment les affaires jointes C-6/90 et C-9/90, Francovich e.a./ Italie, arrêt du 28 mai 1991.

AF. considérant que la collecte massive de données à caractère personnel à des fins commerciales et au nom de la lutte contre le terrorisme et contre la grande criminalité transnationale met à mal les droits des citoyens de l'Union en matière de vie privée et de protection des données à caractère personnel;

Transferts vers les États-Unis au titre de la "sphère de sécurité" des États-Unis

AG. considérant que le cadre juridique des États-Unis en matière de protection des données ne garantit pas un niveau adéquat de protection pour les citoyens de l'Union européenne;

AH. considérant qu'afin de permettre aux responsables de traitements de données de l'Union de transférer des données à caractère personnel vers des entités aux États-Unis, la Commission, dans sa décision 2000/520/CE, a déclaré adéquate la protection assurée par les principes de la "sphère de sécurité" et par les "questions souvent posées" y afférentes, publiés par le ministère du commerce des États-Unis, pour les données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis qui se sont engagées à appliquer les principes de la "sphère de sécurité";

AI. considérant que dans sa résolution du 5 juillet 2000, il a exprimé des doutes et des craintes en ce qui concerne la pertinence des principes de la "sphère de sécurité" et a appelé la Commission à revoir la décision sans délai, à la lumière des expériences acquises et de l'évolution législative éventuelle;

AJ. considérant que, dans le document de travail n° 4 du Parlement européen du 12 décembre 2013 relatif aux activités de surveillance des États-Unis à l'égard des données de l'Union européenne et à leurs implications juridiques éventuelles sur les accords et la coopération transatlantiques, les rapporteurs ont manifesté leurs doutes et leurs inquiétudes quant au caractère approprié de la "sphère de sécurité" et ont demandé à la Commission d'abroger la décision sur la pertinence de la "sphère de sécurité" et de trouver de nouvelles solutions juridiques;

AK. considérant qu'en vertu de la décision 2000/520/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour suspendre les flux de données vers une organisation adhérant aux principes de la "sphère de sécurité" afin de protéger les individus en ce qui concerne le traitement de leurs données personnelles dans les cas où il est fort probable que les principes sont violés ou lorsque la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves;

AL. considérant que la décision 2000/520/CE de la Commission précise également que lorsque les informations recueillies montrent qu'un quelconque organisme chargé de faire respecter les principes ne remplit pas efficacement sa mission, la Commission informe le ministère américain du commerce et, si nécessaire, propose des mesures à prendre en vue d'abroger ou de suspendre ladite décision ou d'en limiter la portée;

AM. considérant que dans ses deux premiers rapports sur l'application des principes de la "sphère de sécurité", publiés en 2002 et 2004, la Commission a relevé plusieurs lacunes au niveau de l'application desdits principes et adressé une série de recommandations aux autorités américaines en vue de corriger ces lacunes;

AN. considérant que dans son troisième rapport de mise en œuvre, du 27 novembre 2013, neuf ans après le deuxième rapport et sans qu'aucune des lacunes recensées dans ce rapport ait été rectifiée, la Commission a relevé d'autres lacunes et faiblesses importantes concernant les principes de la "sphère de sécurité" et a conclu que l'application actuelle ne pouvait se poursuivre; que la Commission a souligné que le vaste accès accordé aux agences de renseignement américaines aux données transférées vers les États-Unis par des entités adhérant aux principes de la "sphère de sécurité" pose d'autres questions majeures quant à la continuité de la protection des données de citoyens européens; que la Commission a adressé 13 recommandations aux autorités américaines et s'est engagée à formuler, d'ici à l'été 2014 et en collaboration avec les autorités américaines, des solutions applicables dans les plus brefs délais et qui constitueront la base d'un examen approfondi du fonctionnement des principes de la "sphère de sécurité";

AO. considérant que du 28 au 31 octobre 2013, une délégation de la commission des libertés civiles, de la justice et des affaires intérieures (commission LIBE) du Parlement européen a rencontré, à Washington D.C., le ministère américain du commerce et la commission fédérale du commerce des États-Unis; que le ministère du commerce a reconnu l'existence d'organisations ayant déclaré adhérer aux principes de la "sphère de sécurité", mais dont le statut n'est pas à jour, ce qui signifie qu'elles ne satisfont pas aux exigences de la "sphère de sécurité" alors qu'elles continuent à recevoir des données à caractère personnel provenant de l'Union européenne; que la commission fédérale du commerce a admis la nécessité de réviser les principes de la "sphère de sécurité" afin de les améliorer, surtout en ce qui concerne les mécanismes de plaintes et de résolution alternative des conflits;

AP. considérant que les principes de la "sphère de sécurité" peuvent être limités "dans la mesure du nécessaire pour répondre aux exigences relatives à la sécurité nationale, l'intérêt public ou le respect des lois"; que, en tant que dérogation à un droit fondamental, celle-ci doit toujours être interprétée de manière restrictive et être limitée à ce qui est nécessaire et proportionné dans une société démocratique, et que la législation doit clairement établir les conditions et garanties permettant de rendre cette restriction légitime; que le champ d'application de cette dérogation aurait dû être précisé par les États-Unis et l'Union européenne, et en particulier par la Commission, afin d'éviter toute interprétation ou application invalidant en substance le droit fondamental à la vie privée et à la protection des données, entre autres; que, par conséquent, une telle dérogation ne doit pas être utilisée d'une manière qui nuirait à ou invaliderait la protection apportée par la charte des droits fondamentaux, la CEDH, la législation de l'Union européenne sur la protection des données et les principes de la "sphère de sécurité"; qu'en cas d'invocation de la dérogation à des fins de sécurité nationale, il est impératif de préciser en vertu du droit national de quel pays;

AQ. considérant que le vaste accès accordé aux agences de renseignement américaines a gravement sapé la confiance transatlantique et a eu des incidences négatives sur la confiance accordée aux organisations américaines actives dans l'Union européenne; que cette situation est encore aggravée par l'absence de moyens de recours judiciaire ou administratif dans le droit américain pour les citoyens de l'Union européenne, en particulier dans des cas d'activités de surveillance menées à des fins de renseignement;

Transferts vers des pays tiers dans le cadre d'une décision relative à la pertinence de la protection

AR. considérant que selon les informations communiquées et les conclusions de l'enquête réalisée par la commission LIBE, les services nationaux de sécurité néozélandais, canadiens et australiens ont été impliqués à un niveau important dans la surveillance de masse des communications électroniques et ont activement coopéré avec les États-Unis dans le cadre du programme dit "Five Eyes" (cinq yeux), et pourraient avoir échangé entre eux des données à caractère personnel de citoyens européens transférées depuis l'Union européenne;

AS. considérant que les décisions 2013/65/UE[76] et 2002/2/CE[77] de la Commission ont déclaré adéquat le niveau de protection garanti respectivement par la loi néozélandaise sur le respect de la vie privée et la loi canadienne relative à la protection des informations à caractère personnel et aux documents électroniques; que les révélations susmentionnées nuisent aussi gravement à la confiance vis-à-vis des systèmes juridiques de ces pays en ce qui concerne la continuité de la protection accordée aux citoyens de l'Union européenne; que la Commission ne s'est pas penchée sur cet aspect;

Transferts fondés sur des clauses contractuelles et d'autres instruments

AT. considérant qu'en vertu de la directive 95/46/CE, les transferts internationaux vers des pays tiers peuvent également être réalisés au titre d'un instrument spécifique dans le cadre duquel le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants;

AU. considérant que ces garanties peuvent notamment résulter de clauses contractuelles appropriées;

AV. considérant que la directive 95/46/CE permet à la Commission de décider que certaines clauses contractuelles types présentent les garanties suffisantes requises par la directive et que sur cette base, la Commission a adopté trois modèles de clauses contractuelles types pour les transferts vers des responsables du traitement et des sous-traitants (et sous-traitants ultérieurs) dans des pays tiers;

AW. considérant qu'en vertu des décisions de la Commission établissant les clauses contractuelles types, les autorités compétentes des États membres peuvent exercer leurs compétences pour suspendre le transfert de données lorsqu'il est établi que le droit auquel l'importateur de données est soumis oblige ce dernier à déroger aux règles pertinentes de protection des données au-delà des restrictions nécessaires dans une société démocratique comme le prévoit l'article 13 de la directive 95/46/CE, lorsque ces obligations risquent d'altérer considérablement les garanties offertes par la législation applicable en matière de protection des données ou les clauses contractuelles types, ou lorsqu'il est fort probable que les clauses contractuelles types figurant dans l'annexe ne sont pas ou ne seront pas respectées et que la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves;

AX. considérant que les autorités nationales de protection des données ont établi des règles d'entreprise contraignantes (REC) en vue de faciliter les transferts internationaux au sein des entreprises multinationales en apportant les garanties adéquates en ce qui concerne

---

[76] JO L 28 du 30.1.2013, p. 12.

[77] JO L 2 du 4.1.2002, p. 13.

la protection de la vie privée et des libertés et droits fondamentaux des personnes ainsi qu'en ce qui concerne l'exercice de ces droits; qu'avant d'être appliquées, les REC doivent être autorisées par les autorités compétentes des États membres, une fois que celles-ci ont évalué leur conformité avec la législation de l'Union sur la protection des données; que les REC applicables aux sous-traitants pour le traitement des données ont été rejetées dans le rapport de la commission LIBE relatif au règlement général sur la protection des données, étant donné qu'elles auraient enlevé au responsable du traitement des données et à la personne concernée tout contrôle sur la juridiction dans laquelle leurs données sont traitées;

AY. considérant qu'en vertu de la compétence qui lui est attribuée par l'article 218 du traité FUE, le Parlement européen a pour responsabilité de contrôler en permanence la valeur des accords internationaux qu'il a approuvés;

Transferts basés sur les accords TFTP et PNR

AZ. considérant que dans sa résolution du 23 octobre 2013, il s'est dit fortement préoccupé par les documents révélés sur les activités de la NSA en ce qui concerne l'accès direct aux données de messagerie financière et aux données connexes, qui constituerait une infraction claire à l'accord TFTP, et notamment à son article premier;

BA. considérant que la surveillance du financement du terrorisme est un outil essentiel dans la lutte contre le financement du terrorisme et la grande criminalité qui permet aux enquêteurs antiterroristes de mettre au jour des liens entre les personnes ciblées par leurs enquêtes et d'autres suspects potentiels en rapport avec des réseaux terroristes plus larges suspectés de financer le terrorisme;

BB. considérant qu'il a demandé à la Commission de suspendre l'accord et a réclamé un accès immédiat à toutes les informations et documents utiles pour ses délibérations; que la Commission n'a accédé à aucune de ces demandes;

BC. considérant qu'à la suite des allégations publiées par les médias, la Commission a décidé d'entamer des consultations avec les États-Unis conformément à l'article 19 de l'accord TFTP; que le 27 novembre 2013, la commissaire Malmström a informé la commission LIBE qu'après avoir rencontré les autorités américaines et compte tenu des réponses apportées par celles-ci dans leurs lettres et pendant leurs réunions, la Commission avait décidé de ne pas poursuivre les consultations au motif qu'aucun élément ne démontrait que le gouvernement américain avait agi contrairement aux dispositions de l'accord et que les États-Unis avaient fourni la garantie écrite qu'ils n'avaient procédé à aucune collecte de données directes qui contreviendrait aux dispositions de l'accord TFTP; qu'il n'est pas certain que les autorités américaines aient contourné l'accord en accédant à ces données par d'autres moyens, tel qu'indiqué dans la lettre du 18 septembre 2013 des autorités américaines[78];

BD. considérant que pendant son séjour à Washington du 28 au 31 octobre 2013, la délégation LIBE a rencontré le département du Trésor des États-Unis; que le Trésor

---

[78] La lettre mentionne que le gouvernement des États-Unis recherche et obtient des informations financières [...] (qui) sont collectées via des voies réglementaires, des mesures d'application de la loi, des voies diplomatiques et des activités de renseignement ainsi que des échanges avec des partenaires étrangers [...] le gouvernement américain a recours au TFTP pour obtenir des données SWIFT que nous ne pouvons obtenir par d'autres sources.

américain a affirmé n'avoir eu, depuis l'entrée en vigueur de l'accord TFTP, aucun accès à des données SWIFT dans l'Union européenne, si ce n'est dans le cadre de l'accord TFTP; que le département du Trésor a refusé de commenter la possibilité que des données SWIFT aient été consultées en dehors de l'accord TFTP par un autre organisme gouvernemental ou ministère américain, ou que l'administration américaine ait eu connaissance des activités de surveillance de masse de la NSA; que le 18 décembre 2013, M. Glenn Greenwald a déclaré dans le cadre de l'enquête menée par la commission LIBE que la NSA et le GCHQ avaient ciblé les réseaux SWIFT;

BE. considérant que le 13 novembre 2013, les autorités de protection des données belges et néerlandaises ont décidé d'organiser une enquête conjointe sur la sécurité des réseaux de paiement de l'organisation SWIFT afin de contrôler si des tiers ont pu accéder de façon non autorisée ou illicite aux données bancaires de citoyens européens[79];

BF. considérant que selon l'examen conjoint de l'accord UE-États-Unis sur les dossiers des passagers aériens, le ministère américain de la sécurité intérieure a divulgué à 23 reprises des données PNR à la NSA, au cas par cas, dans le cadre d'affaires liées à la lutte contre le terrorisme, dans le respect des conditions précises de l'accord;

BG. considérant que l'examen conjoint ne fait pas mention du fait qu'en cas de traitement de données à caractère personnel à des fins de renseignement, en vertu du droit américain, les ressortissants non américains ne bénéficient d'aucune voie judiciaire ou administrative pour protéger leurs droits et que les protections constitutionnelles ne sont accordées qu'aux ressortissants américains; que cette absence de droits judiciaires ou administratifs annule les protections prévues pour les citoyens de l'Union dans l'accord PNR existant;

Transferts basés sur l'accord entre l'Union européenne et les États-Unis sur l'entraide judiciaire en matière pénale

BH. considérant que l'accord entre l'Union européenne et les États-Unis sur l'entraide judiciaire en matière pénale du 6 juin 2003[80] est entré en vigueur le 1er février 2010 et a pour but de faciliter la coopération entre l'Union européenne et les États-Unis afin de lutter plus efficacement contre la criminalité, en tenant dûment compte des droits des personnes et de l'état de droit;

Accord-cadre sur la protection des données dans le domaine de la coopération policière et judiciaire (l'"accord-cadre")

BI. considérant que cet accord général a pour finalité d'établir le cadre juridique pour tous les transferts de données à caractère personnel entre l'Union européenne et les États-Unis dans le seul but de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale; que les négociations ont été autorisées par le Conseil le 2 décembre 2010; que cet accord revêt une importance primordiale et contribuerait à faciliter les transferts de données dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale;

---

79 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

80 JO L 181 du 19.7.2003, p. 25.

BJ. considérant que cet accord devrait contenir des principes clairs et précis, juridiquement contraignants, en matière de traitement des données, et devrait notamment reconnaître le droit des citoyens de l'Union d'accéder sur le plan judiciaire à leurs données à caractère personnel aux États-Unis, et de les rectifier et de les effacer, ainsi que le droit à des moyens de recours judiciaire ou administratif efficaces pour les citoyens de l'Union aux États-Unis et à une surveillance indépendante des activités de traitement de données;

BK. considérant que dans sa communication du 27 novembre 2013, la Commission a indiqué que l'accord-cadre devrait garantir un niveau élevé de protection des citoyens des deux côtés de l'Atlantique et devrait renforcer la confiance des Européens dans les échanges de données entre l'Union européenne et les États-Unis, en constituant ainsi une base permettant de développer la coopération et le partenariat entre l'Union et les États-Unis en matière de sécurité;

BL. considérant que les négociations sur l'accord n'ont pas progressé en raison de la persistance du gouvernement américain à refuser de reconnaître aux citoyens de l'Union le droit effectif à des moyens de recours administratif et judiciaire et de l'intention d'inclure de vastes dérogations aux principes de protection des données qui figureront dans l'accord, tels que la limitation des finalités, la conservation des données ou les transferts ultérieurs, nationaux ou à l'étranger;

Réforme dans le domaine de la protection des données

BM. considérant que le cadre juridique de l'Union européenne en matière de protection des données fait actuellement l'objet d'un réexamen en vue de mettre en place un système complet, cohérent, moderne et solide pour l'ensemble des activités de traitement de données dans l'Union; que la Commission a présenté en janvier 2012 un ensemble de propositions législatives: un règlement général sur la protection des données[81], qui remplacera la directive 95/46/CE et établira une législation uniforme dans toute l'Union, et une directive[82] qui établira un cadre harmonisé pour l'ensemble des activités de traitement de données réalisées par les autorités répressives à des fins répressives et réduira les divergences actuelles entre les législations nationales;

BN. considérant que le 21 octobre 2013, la commission LIBE a adopté ses rapports législatifs sur les deux propositions ainsi qu'une décision concernant l'ouverture de négociations avec le Conseil en vue de faire adopter les instruments juridiques avant la fin de la présente législature;

BO. considérant que bien que le Conseil européen des 24 et 25 octobre 2013 ait réclamé l'adoption en temps voulu d'un cadre général rigoureux de l'Union sur la protection des données en vue de renforcer la confiance des citoyens et des entreprises à l'égard de l'économie numérique, il n'est toujours pas parvenu, après deux années de délibérations, à définir une approche globale concernant le règlement général sur la protection des données et la directive[83];

Sécurité informatique et informatique en nuage

---

81 COM(2012)0011 du 25.1.2012.

82 COM(2012)0010 du 25.1.2012.

83 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/fr/ec/139210.pdf

BP. considérant que sa résolution du 10 décembre 2013 mentionnée ci-dessus souligne le potentiel économique offert par l'informatique en nuage pour la croissance et l'emploi; que, selon les prévisions, la valeur économique globale du marché de l'informatique en nuage équivaut à 207 milliards de dollars américains par an d'ici à 2016, soit le double de sa valeur en 2012;

BQ. considérant que le niveau de protection des données dans un environnement d'informatique en nuage ne doit pas être moins élevé à celui exigé dans un autre cadre de traitement de données; que le droit de l'Union en matière de protection des données, neutre sur le plan technologique, s'applique déjà pleinement aux services d'informatique en nuage actifs dans l'Union européenne;

BR. considérant que les activités de surveillance de masse donnent aux agences de renseignement l'accès aux données à caractère personnel stockées ou autrement traitées par les particuliers de l'Union européenne dans le cadre d'accords de services en nuage avec les grands fournisseurs d'informatique en nuage américains; que les services de renseignement américains ont accédé à des données à caractère personnel stockées ou autrement traitées dans des serveurs localisés sur le sol européen en exploitant les réseaux internes de Yahoo et Google; que de telles activités constituent une violation des obligations internationales et des normes européennes en matière de droits fondamentaux, dont font partie le droit à la vie privée et familiale, la confidentialité des communications, la présomption d'innocence, la liberté d'expression, la liberté d'information, la liberté de réunion et d'association et la liberté d'entreprise; qu'il n'est pas impossible que les services de renseignement aient également accédé à des informations stockées dans des services en nuage par les autorités ou entreprises publiques et les institutions des États membres;

BS. considérant que les services de renseignement américains appliquent une politique de sape systématique des protocoles et produits cryptographiques afin d'être en mesure d'intercepter même les communications cryptées; que l'agence de sécurité nationale des États-Unis a collecté un grand nombre de "vulnérabilités jour zéro" – à savoir des vulnérabilités informatiques en matière de sécurité dont le public et le fournisseur du produit n'ont pas encore connaissance; que de telles activités mettent considérablement à mal les efforts mondiaux visant à améliorer la sécurité informatique;

BT. considérant que le fait que les agences de renseignement aient eu accès aux données à caractère personnel des utilisateurs de services en ligne a fortement dégradé la confiance des citoyens dans ces services, ce qui a donc un effet néfaste sur les entreprises investissant dans le développement de nouveaux services qui ont recours aux "données massives" et de nouvelles applications, telles que l'internet des objets;

BU. considérant que les fournisseurs de technologies de l'information proposent souvent des produits dont la sécurité informatique n'a pas été convenablement testée ou qui parfois disposent de portes dérobées intégrées à dessein par le fournisseur; que l'absence de règles en matière de responsabilité des fournisseurs de logiciels a conduit à une telle situation, qui est exploitée par les services de renseignement, mais qui ouvre aussi la voie au risque d'attaques d'autres entités;

BV. considérant qu'il est essentiel que les entreprises fournissant ce type de nouveaux services et de nouvelles applications respectent les règles relatives à la protection des

données et à la vie privée des utilisateurs dont les données sont collectées, traitées et analysées, afin de maintenir la confiance des citoyens à un niveau élevé;

Contrôle démocratique des services de renseignement

BW. considérant que, dans les sociétés démocratiques, les services de renseignement sont dotés de pouvoirs et moyens spéciaux pour protéger les droits fondamentaux, la démocratie et l'état de droit, les droits des citoyens et l'État contre les menaces intérieures et extérieures, et font l'objet d'un contrôle démocratique et judiciaire; qu'ils jouissent de capacités et de pouvoirs spéciaux uniquement à cet effet; que ces pouvoirs doivent être employés dans les limites du cadre juridique imposé par les droits fondamentaux, la démocratie et l'état de droit et que leur application doit être strictement contrôlée, sans quoi ils perdent leur légitimité et risquent de porter atteinte à la démocratie;

BX. considérant que, si un certain degré de confidentialité est accordé aux services de renseignements pour éviter la mise en péril des opérations en cours, la divulgation des modus operandi ou la mise en danger des agents, cette confidentialité ne peut outrepasser ou exclure les règles relatives au contrôle et à l'examen démocratiques et judiciaires de leurs activités, ainsi que les règles de transparence, notamment en ce qui concerne le respect des droits fondamentaux et de l'état de droit, qui sont autant d'éléments essentiels des sociétés démocratiques;

BY. considérant que la plupart des mécanismes et organes de contrôle nationaux existants ont été créés ou réorganisés dans les années 1990 et n'ont pas nécessairement été adaptés aux rapides progrès technologiques et évolutions politiques de la décennie écoulée, qui ont conduit les services de renseignements à coopérer davantage à l'échelle internationale, notamment par l'échange à grande échelle de données à caractère personnel, ce qui crée souvent une confusion des genres entre renseignement et répression;

BZ. considérant que le contrôle démocratique des services de renseignement est toujours effectué uniquement au niveau national, malgré l'accroissement des échanges d'informations entre les États membres de l'Union ainsi qu'entre les États membres et les pays tiers; qu'il existe un écart grandissant entre, d'une part, le niveau de coopération internationale et, d'autre part, les capacités de contrôle limitées au niveau national, ce qui engendre un contrôle démocratique insuffisant et inefficace;

CA. considérant que les organes de contrôle nationaux n'ont souvent pas pleinement accès aux renseignements reçus des services étrangers, ce qui est susceptible de créer un "entre-deux" où les échanges internationaux d'informations peuvent avoir lieu sans contrôle approprié; que ce problème est aggravé par la règle dite du "tiers service" ou le principe du "contrôle par l'entité d'origine", qui vise à permettre à l'entité dont émanent les informations de décider de la diffusion ou non de ses informations sensibles à d'autres entités mais qui est parfois malheureusement interprétée en ce sens qu'elle s'applique aussi au contrôle des services destinataires;

CB. considérant que les initiatives de réforme en matière de transparence des secteurs public et privé sont essentielles pour donner confiance au public dans les activités des services de renseignement; que les systèmes juridiques ne devraient pas empêcher les entreprises de rendre publique la façon dont elle traite tous les types de requêtes des gouvernements

et d'injonctions des tribunaux demandant l'accès aux données de leurs utilisateurs, y compris la divulgation d'informations globales sur le nombre de requêtes et d'injonctions acceptées et rejetées;

Conclusions principales

1. estime que les récentes révélations faites dans la presse par des lanceurs d'alerte et des journalistes, ainsi que les témoignages d'experts recueillis pendant cette enquête, les aveux des autorités et l'insuffisance de la réaction face à ces allégations, ont permis d'obtenir des preuves irréfutables de l'existence de systèmes vastes, complexes et technologiquement très avancés conçus par les services de renseignement des États-Unis et de certains États membres dans le but de collecter, de stocker et d'analyser les données de communication, y compris les données de contenu, et les données et métadonnées de localisation des citoyens du monde entier, à une échelle sans précédent, sans aucun discernement et sans se baser sur des soupçons;

2. appelle plus particulièrement l'attention sur les programmes de renseignement de la NSA permettant la surveillance de masse des citoyens de l'Union européenne grâce à l'accès direct aux serveurs centraux des grandes entreprises américaines du secteur de l'internet (programme PRISM), à l'analyse de contenus et de métadonnées (programme Xkeyscore), au contournement du cryptage en ligne (BULLRUN), et à l'accès aux réseaux informatiques et téléphoniques et aux données de localisation, mais aussi sur les systèmes de l'agence de renseignement britannique GCHQ, notamment son activité de surveillance en amont (programme Tempora) et son programme de décryptage (Edgehill), les attaques ciblées "de l'homme du milieu" sur des systèmes informatiques (programmes Quantum et Foxacid) et la collecte et la conservation de quelque 200 millions de SMS par jour (programme Dishfire);

3. prend note des allégations de piratage ou d'exploitation des systèmes de Belgacom par l'agence de renseignement britannique GCHQ; constate que Belgacom a indiqué ne pas être en mesure de confirmer ou d'infirmer que les institutions de l'Union européenne étaient ciblées ou touchées, et a affirmé que les logiciels malveillants utilisés étaient des logiciels extrêmement complexes dont le développement et l'utilisation ont nécessité d'importants moyens financiers et humains dont n'auraient pas pu disposer des entités privées ou des pirates;

4. souligne que la confiance a été profondément mise à mal, à savoir la confiance entre les deux partenaires transatlantiques, la confiance entre les citoyens et leurs gouvernements, la confiance dans le fonctionnement des institutions démocratiques des deux côtés de l'Atlantique, la confiance à l'égard du respect de l'état de droit et la confiance dans la sécurité des services et des communications informatiques; pense que pour restaurer la confiance à tous ces égards, il est indispensable d'adopter un plan d'intervention immédiat et global prévoyant un ensemble de mesures soumises au contrôle des citoyens;

5. note que plusieurs gouvernements affirment que ces programmes de surveillance de masse sont nécessaires à la lutte contre le terrorisme; dénonce fermement le terrorisme, mais est convaincu que la lutte contre le terrorisme ne peut en aucun cas justifier l'existence de programmes de surveillance de masse non ciblés, secrets, voire illégaux; estime que de tels programmes sont incompatibles avec les principes de nécessité et de proportionnalité en vigueur dans les sociétés démocratiques;

6. réaffirme la ferme conviction de l'Union selon laquelle il convient d'établir un juste équilibre entre les mesures de sécurité et la protection des libertés civiles et des droits fondamentaux, tout en veillant au respect le plus strict de la vie privée et de la protection des données;

7. considère que, face à une collecte de données d'une telle ampleur, on peut sérieusement douter que ces mesures ne soient motivées que par la seule lutte contre le terrorisme, étant donné qu'elles supposent le recueil de toutes les données possibles de l'ensemble des citoyens; signale par conséquent l'existence possible d'autres motifs, notamment l'espionnage politique et économique, qu'il faut entièrement dissiper;

8. s'interroge sur la compatibilité des activités d'espionnage économique de masse de certains États membres avec le droit du marché intérieur et de la concurrence de l'Union européenne consacré aux titres I et VII du traité sur le fonctionnement de l'Union européenne; réaffirme le principe de coopération loyale établi à l'article 4, paragraphe 3, du traité sur l'Union européenne et le principe selon lequel que les États membres "s'abstiennent de toute mesure susceptible de mettre en péril la réalisation des objectifs de l'Union";

9. relève que les traités internationaux et la législation de l'Union européenne et des États-Unis, ainsi que les mécanismes de contrôle nationaux, n'ont prévu ni les systèmes de contre-pouvoir, ni le contrôle démocratique nécessaires;

10. condamne le recueil à grande échelle, systémique et aveugle des données à caractère personnel de personnes innocentes, qui comprennent souvent des informations personnelles intimes; souligne que les systèmes de surveillance de masse sans discernement mis en place par les services de renseignement constituent une grave entrave aux droits fondamentaux des citoyens; souligne que le respect de la vie privée n'est pas un droit de luxe, mais constitue la pierre angulaire de toute société libre et démocratique; souligne par ailleurs que la surveillance de masse a des répercussions potentiellement graves sur la liberté de la presse, la liberté de pensée et la liberté d'expression, ainsi que sur la liberté de réunion et d'association, et qu'elle entraîne un risque élevé d'utilisation abusive des informations collectées à l'encontre d'adversaires politiques; insiste sur le fait que ces activités de surveillance de masse donnent également lieu à des actions illégales de la part des services de renseignement et qu'elles soulèvent des questions au sujet de l'extraterritorialité des législations nationales;

11. juge capital de protéger le secret professionnel des avocats, des journalistes, des médecins et des autres professions réglementées contre les activités de surveillance de masse; souligne en particulier que toute incertitude concernant la confidentialité des communications entres les avocats et leurs clients pourrait avoir des incidences négatives sur le droit d'accès des citoyens de l'Union européenne à l'assistance juridique et à la justice, ainsi que le droit à un procès équitable;

12. estime que les programmes de surveillance constituent une nouvelle étape vers la mise en place d'un État "ultrapréventif", s'éloignant du modèle établi du droit pénal en vigueur dans les sociétés démocratiques, selon lequel toute atteinte aux droits fondamentaux d'un suspect nécessite l'autorisation d'un juge ou d'un procureur, en l'existence de soupçons raisonnables, et doit impérativement être régie par la loi, pour y substituer un mélange d'activités de répression et de renseignement avec des garanties juridiques floues et affaiblies, allant bien souvent à l'encontre des freins et contrepoids

démocratiques et des droits fondamentaux, en particulier de la présomption d'innocence; rappelle à cet égard la décision de la Cour constitutionnelle fédérale allemande[84] sur l'interdiction du recours au profilage préventif (präventive Rasterfahndung) en l'absence d'éléments démontrant la mise en péril d'autres droits importants et juridiquement protégés, selon laquelle une menace générale ou des tensions internationales ne suffisent pas à justifier de telles mesures;

13. est convaincu que les législations et tribunaux secrets constituent une violation de l'état de droit; souligne que les arrêts des cours ou tribunaux et les décisions d'autorités administratives d'un pays tiers autorisant, directement ou indirectement, le transfert de données personnelles, ne doivent en aucun cas être reconnus ou appliqués, sauf si un traité d'entraide judiciaire ou un accord international est en vigueur entre le pays tiers demandeur et l'Union ou un État membre, et sous réserve de l'accord préalable de l'autorité de contrôle compétente; rappelle que les arrêts rendus par des cours ou tribunaux secrets et les décisions émises par des autorités administratives de pays non membres de l'Union autorisant de manière confidentielle, directement ou indirectement, des activités de surveillance, ne doivent ni être reconnus, ni appliqués;

14. souligne que les préoccupations susmentionnées sont exacerbées par la rapidité des évolutions technologiques et sociétales, les appareils internet et mobiles étant omniprésents dans la vie quotidienne moderne ("informatique ubiquitaire") et le modèle commercial de la plupart des entreprises du secteur de l'internet reposant sur le traitement de données à caractère personnel; estime que l'ampleur de ce problème est sans précédent; constate que l'on pourrait assister à une utilisation abusive des infrastructures de collecte massive et de traitement des données en cas de changement de régime politique;

15. observe qu'il n'existe aucune garantie, que ce soit pour les institutions publiques européennes ou pour les citoyens, que leur sécurité informatique ou leur vie privée puisse être protégée des attaques d'intrus bien équipés ("pas de sécurité informatique à 100 %"); note que pour pouvoir jouir d'une sécurité informatique maximale, les Européens doivent accepter de consacrer suffisamment de moyens, humains et financiers, à la préservation de l'indépendance et de l'autosuffisance de l'Europe dans le domaine des technologies de l'information;

16. rejette vivement l'idée selon laquelle toutes les questions liées aux programmes de surveillance de masse relèveraient strictement de la sécurité nationale et, dès lors, de l'unique compétence des États membres; réaffirme que les États membres doivent respecter pleinement la législation de l'Union et la convention européenne des droits de l'homme lorsqu'ils agissent pour assurer leur sécurité nationale; rappelle une récente décision de la Cour de justice selon laquelle "bien qu'il appartienne aux États membres d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une décision concerne la sûreté de l'État ne saurait entraîner l'inapplicabilité du droit de l'Union"[85]; rappelle par ailleurs qu'il y va de la protection de la vie privée de tous les citoyens de l'Union européenne, de même que de la sécurité et de la fiabilité de tous les réseaux de communication de l'Union; pense par conséquent qu'une discussion et une action au niveau de l'Union européenne ne sont pas seulement légitimes, mais nécessaires pour l'autonomie de l'Union;

---

84 N° 1 BvR 518/02 du 4 avril 2006.

85 Arrêt du 4 juin 2013 dans l'affaire C-300/11, ZZ contre Secretary of State for the Home Department.

17. félicite les institutions et les experts ayant contribué à cette enquête; déplore le fait que les autorités de plusieurs États membres aient refusé de coopérer dans l'enquête réalisée par le Parlement européen au nom de ses citoyens; salue l'ouverture dont ont fait preuve plusieurs membres du Congrès et des parlements nationaux;

18. est conscient que dans des délais aussi serrés, seule une enquête préliminaire sur toutes les questions soulevées depuis juillet 2013 a pu être réalisée; reconnaît à la fois l'ampleur des révélations dont il est question et leur caractère permanent; adopte par conséquent une approche à long terme consistant en une série de propositions spécifiques ainsi qu'en un mécanisme prévoyant un suivi au cours de la prochaine législature, afin de faire en sorte que les conclusions formulées continuent demeurent des priorités politiques majeures de l'Union;

19. compte demander à la nouvelle Commission qui sera désignée après les élections européennes de mai 2014 de prendre des engagements politiques forts en vue de mettre en œuvre les propositions et recommandations de l'enquête;

Recommandations

20. demande aux autorités américaines et aux États membres de l'Union européenne d'interdire les activités de surveillance de masse aveugle, s'ils ne l'ont pas déjà fait;

21. exhorte tous les États membres de l'Union, en particulier ceux qui participent aux programmes "9-eyes" et "14-eyes"[86], à procéder à un examen complet, et à la révision au besoin, de leurs législations et pratiques régissant les activités des services de renseignement afin de s'assurer qu'elles font l'objet d'un contrôle parlementaire et judiciaire et sont soumises à la vigilance des citoyens, qu'elles respectent les principes de légalité, de nécessité, de proportionnalité, de traitement équitable, d'information de l'utilisateur et de transparence, notamment en s'appuyant sur le recueil de bonnes pratiques des Nations unies et sur les recommandations de la Commission de Venise, et qu'elles sont conformes aux normes de la convention européenne des droits de l'homme et aux obligations des États membres en matière de droits fondamentaux, notamment en ce qui concerne la protection des données, le respect de la vie privée et la présomption d'innocence;

22. invite tous les États membres de l'Union européenne et en particulier, compte tenu de sa résolution du 4 juillet 2013 et de ses auditions d'enquête, le Royaume-Uni, la France, l'Allemagne, la Suède, les Pays-Bas et la Pologne à veiller à ce que leur cadre législatif et leurs mécanismes de contrôle, actuels et à venir, applicables aux activités des services de renseignement soient conformes aux normes de la convention européenne des droits de l'homme et au droit de l'Union européenne en matière de protection des données; invite ces États membres à faire la lumière sur les allégations concernant des activités de surveillance massive, y compris la surveillance massive des communications transfrontalières, la surveillance non ciblée des communications par câble, les accords éventuels passés entre les services de renseignement et des entreprises de télécommunications concernant l'accès aux données personnelles et leur échange et l'accès aux câbles transatlantiques, la présence sur le territoire de l'Union européenne de personnels et d'équipements de renseignement américains sans contrôle sur les

[86] Le "programme "9-eyes" englobe les États-Unis, le Royaume-Uni, le Canada, l'Australie, la Nouvelle-Zélande, le Danemark, la France, la Norvège et les Pays-Bas; le programme "14-eyes" comprend aussi, outre ces pays, l'Allemagne, la Belgique, l'Italie, l'Espagne et la Suède.

opérations de surveillance, et leur compatibilité avec la législation de l'Union; invite les parlements nationaux desdits pays à intensifier la coopération de leurs organes de surveillance des services de renseignement au niveau européen;

23. invite le Royaume-Uni, en particulier, compte tenu des nombreuses informations fournies par les médias faisant état d'une surveillance de masse par le service de renseignement GHCQ, à réviser son cadre juridique actuel consistant en l'"interaction complexe" de trois actes législatifs distincts – la loi de 1998 sur les droits de l'homme, la loi de 1994 sur les services de renseignement et la loi de 2000 sur la règlementation des pouvoirs d'enquête;

24. prend acte de la révision de la loi néerlandaise de 2002 sur le renseignement et la sécurité (rapport de la commission Dessens du 2 décembre 2013); soutient les recommandations de la commission de révision visant à augmenter la transparence du fonctionnement des services de renseignement néerlandais et à renforcer le contrôle et la supervision à l'égard de ces derniers; prie les Pays-Bas de s'abstenir d'étendre les pouvoirs des services de renseignement de façon à permettre de procéder également à une surveillance systématique et à grande échelle des communications par câble de citoyens innocents, en particulier compte tenu du fait que l'un des plus importants points d'échange internet (AMS-IX) se situe à Amsterdam; appelle à la prudence quant à la définition du mandat et des capacités de la nouvelle unité commune pour le renseignement d'origine électronique et informatique, ainsi qu'à l'égard de la présence et des activités de membres des services de renseignement états-uniens sur le territoire des Pays-Bas;

25. invite les États membres, y compris lorsqu'ils sont représentés par leurs services de renseignement, à s'abstenir d'accepter des données provenant de pays tiers et ayant été collectées illégalement, ainsi que d'accepter que des gouvernements ou agences de pays tiers effectuent sur leur territoire des activités de surveillance contraires au droit national ou ne satisfaisant pas aux garanties juridiques spécifiées dans les instruments internationaux ou européens, notamment la protection des droits de l'homme au titre du traité UE, de la CEDH et de la charte des droits fondamentaux de l'Union européenne;

26 demande que tous les services secrets cessent d'intercepter massivement et d'exploiter les images de webcams; invite les États membres à mener une enquête approfondie pour savoir si, comment et dans quelle mesure leurs services secrets respectifs ont pris part à la collecte et au traitement des images de webcams et à supprimer toutes les images enregistrées dans le cadre des programmes de surveillance de masse;

27. exhorte les États membres à satisfaire immédiatement à l'obligation positive qui leur incombe au titre de la convention européenne des droits de l'homme de protéger leurs citoyens des activités de surveillance contraires aux dispositions de la convention, y compris lorsque ces activités visent à garantir la sécurité nationale, réalisées par des pays tiers ou par leurs propres services de renseignement et à veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale du droit d'un pays tiers;

28. invite le secrétaire général du Conseil de l'Europe à lancer la procédure au titre de l'article 52 qui prévoit que "[t]oute Haute Partie contractante fournira sur demande du Secrétaire Général du Conseil de l'Europe les explications requises sur la manière dont son droit interne assure l'application effective de toutes les dispositions de cette Convention";

29. invite les États membres à prendre immédiatement les mesures nécessaires, y compris en matière judiciaire, contre les violations de leur souveraineté, et, par là-même, contre les violations du droit public international général commises par l'intermédiaire des programmes de surveillance de masse; exhorte également les États membres à faire usage de toutes les mesures internationales à leur disposition pour défendre les droits fondamentaux des citoyens européens, notamment en déclenchant la procédure de plainte interétatique prévue par l'article 41 du pacte international relatif aux droits civils et politiques (PIDCP);

30. invite les États membres à mettre en place des mécanismes efficaces par lesquels les personnes responsables des programmes de surveillance (de masse) qui enfreignent l'État de droit et les droits fondamentaux des citoyens doivent répondre des abus de pouvoir qu'ils ont commis;

31. invite les États-Unis à réviser sans tarder leur législation afin de la rendre conforme au droit international, à reconnaître le droit à la vie privée et les autres droits des citoyens de l'Union européenne, à prévoir des moyens de recours judiciaire pour les citoyens de l'Union, à mettre les droits des citoyens de l'Union sur un pied d'égalité avec ceux des citoyens états-uniens et à signer le protocole optionnel permettant aux particuliers de soumettre des plaintes au titre du PIDCP;

32. salue, à cet égard, les observations et la directive présidentielle de Barack Obama, président des États-Unis, du 17 janvier 2014, y voyant un progrès vers la limitation des autorisations d'utiliser la surveillance et le traitement de données pour des motifs de sécurité nationale, et vers le traitement égal par la communauté états-unienne du renseignement des informations personnelles de tous, sans distinction liée à la nationalité ou au lieu de résidence; awaits, however, in the context of the EU-US relationship, further specific steps which will, most importantly, strengthen trust in transatlantic data transfers and provide for binding guarantees for enforceable privacy rights of EU citizens, as outlined in detail in this report;

33. souligne ses vives inquiétudes face aux travaux en cours au sein du comité de la convention cybercriminalité du Conseil de l'Europe sur l'interprétation de l'article 32 de la convention cybercriminalité du 23 novembre 2001 (convention de Budapest) concernant l'accès transfrontalier à des données informatiques stockées avec autorisation ou lorsque le public peut les consulter, et s'oppose à la conclusion de tout protocole additionnel et à la formulation de toute orientation visant à élargir le champ d'application de cette disposition au-delà du régime établi par la convention, qui constitue déjà une exception de taille au principe de territorialité, en ce qu'il pourrait donner aux autorités répressives la possibilité d'accéder librement à distance aux serveurs et aux systèmes informatiques situés dans d'autres juridictions sans avoir recours aux accords multilatéraux et aux autres instruments de coopération judiciaire mis en place pour garantir les droits fondamentaux des personnes physiques, y compris la protection des données et l'application régulière de la loi, et notamment la convention n° 108 du Conseil de l'Europe;

34. invite la Commission à réaliser, avant juillet 2014, une évaluation de l'applicabilité du règlement (CE) n° 2271/96 aux cas de conflits de législations lors de transferts de données à caractère personnel;

35. demande à l'Agence des droits fondamentaux d'effectuer des recherches approfondies sur la protection des droits fondamentaux dans le contexte de la surveillance, et notamment sur l'actuelle situation juridique des citoyens de l'Union européenne pour ce qui touche aux voies de recours juridictionnelles dont ils disposent à l'égard de ces pratiques;

Transferts internationaux de données

Le cadre juridique américain en matière de protection des données et la "sphère de sécurité" des États-Unis

36. observe que les entreprises qui ont été identifiées dans les révélations faites aux médias comme étant impliquées dans la surveillance de masse à grande échelle des personnes concernées dans l'Union effectuée par la NSA sont des entreprises qui ont affirmé adhérer aux principes de la "sphère de sécurité" et que cette sphère est l'instrument juridique utilisé pour le transfert des données européennes à caractère personnel vers les États-Unis (par exemple Google, Microsoft, Yahoo!, Facebook, Apple, LinkedIn); est préoccupé par le fait que ces entreprises n'ont pas crypté les flux d'informations et de communications entre leurs centres de données, ce qui a permis aux services de renseignement d'intercepter les informations; salue les déclarations de certaines entreprises américaines faites en réponse à ces révélations, selon lesquelles elles accélèreraient les projets de mise en œuvre de cryptage des flux de données circulant entre leurs centres de données mondiaux;

37. considère que l'accès à grande échelle par les agences de renseignement américaines aux données européennes à caractère personnel traitées par la "sphère de sécurité" ne répond pas aux critères de dérogation visés au point "sûreté de l'État";

38. estime qu'étant donné que, dans les circonstances actuelles, les principes de la "sphère de sécurité" ne permettent pas d'assurer une protection suffisante pour les citoyens de l'Union, ces transferts doivent être réalisés dans le cadre d'autres instruments, comme des clauses contractuelles ou des règles d'entreprise contraignantes, à condition que ces instruments présentent des garanties et des protections spécifiques et ne soient pas contournés par d'autres cadres juridiques;

39. est d'avis que la Commission n'a pas pris les mesures nécessaires pour remédier aux faiblesses bien connues dont souffre actuellement la mise en œuvre de la "sphère de sécurité";

40. invite la Commission à présenter des mesures prévoyant la suspension immédiate de sa décision 2000/520/CE, qui déclare la pertinence de la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes publiées par le ministère du commerce des États-Unis d'Amérique; invite par conséquent les autorités des États-Unis à présenter une proposition de nouveau cadre pour les transferts de données à caractère personnel de l'Union européenne vers les États-Unis, qui respecte les exigences de protection des données de la législation de l'Union et garantisse un degré de protection adéquat ;

41. invite les autorités compétentes des États membres, en particulier les autorités chargées de la protection des données, à faire usage de leurs compétences existantes pour suspendre sans attendre les flux de données à destination de toute organisation ayant

adhéré aux principes de la "sphère de sécurité" américaine et à exiger que ces flux de données ne soient réalisés que dans le cadre d'autres instruments, pour autant qu'ils contiennent les garanties nécessaires en ce qui concerne la protection de la vie privée et les droits et libertés fondamentaux des individus;

42. invite la Commission à présenter d'ici décembre 2014 une évaluation complète du cadre américain en matière de respect de la vie privée, portant sur les activités commerciales, policières et de renseignement, ainsi que des recommandations concrètes en l'absence de loi générale sur la protection des données aux États-Unis; encourage la Commission à travailler de concert avec les autorités des États-Unis afin d'établir un cadre juridique garantissant un degré élevé de protection des personnes eu égard à la protection de leurs données à caractère personnel lorsqu'elles sont transférées aux États-Unis et à veiller à l'équivalence des cadres européen et américain de respect de la vie privée;

Transferts vers d'autres pays tiers dans le cadre de la décision relative à la pertinence de la protection

43. rappelle que la directive 95/46/CE dispose que les transferts vers un pays tiers de données à caractère personnel ne peuvent avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la directive, le pays tiers en question assure un niveau de protection adéquat, l'objet de cette disposition étant d'assurer la continuité de la protection offerte par la législation européenne en matière de protection des données lorsque des données à caractère personnel sont transférées hors de l'Union européenne;

44. rappelle que la directive 95/46/CE précise également que le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de telles opérations; dans le même ordre d'idées, rappelle que ladite directive confère également à la Commission des compétences d'exécution pour déclarer qu'un pays tiers assure un niveau de protection adéquat au regard des critères établis par la directive 95/46/CE; souligne que la directive 95/46/CE permet aussi à la Commission de déclarer qu'un pays tiers n'assure pas le niveau de protection adéquat;

45. rappelle que, dans ce dernier cas, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause, et que la Commission doit engager des négociations en vue de remédier à cette situation;

46. invite la Commission et les États membres à déterminer sans tarder si le niveau de protection adéquat assuré par la loi de Nouvelle-Zélande sur la vie privée et par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, tel que déclaré par les décisions 2013/65/UE du 19 décembre 2012 et 2002/2/CE de la Commission, a été affecté par la participation des agences nationales de renseignement de ces pays à la surveillance de masse des citoyens de l'Union européenne et, le cas échéant, à prendre les mesures appropriées pour suspendre ou annuler les décisions relatives à la pertinence de la protection; invite également la Commission à examiner la situation d'autres pays ayant fait l'objet d'une évaluation du caractère adéquat du niveau de protection assuré; attend de la Commission qu'elle rende compte au Parlement de ses observations sur les pays mentionnés plus haut avant décembre 2014;

Transferts fondés sur des clauses contractuelles et d'autres instruments

47. rappelle que les autorités nationales chargées de la protection des données ont indiqué que ni les clauses contractuelles types, ni les règles d'entreprise contraignantes n'étaient formulées en prenant en considération les situations d'accès aux données à caractère personnel à des fins de surveillance de masse, et que cet accès ne serait pas conforme aux clauses dérogatoires des clauses contractuelles ou des règles d'entreprise contraignantes qui concernent des dérogations exceptionnelles répondant à un intérêt légitime dans une société démocratique, lorsqu'elles sont nécessaires et proportionnées;

48. invite les États membres à interdire ou à suspendre les flux de données vers des pays tiers, fondés sur des clauses contractuelles types, des clauses contractuelles ou des règles d'entreprise contraignantes autorisées par les autorités nationales compétentes lorsqu'il est probable que la loi à laquelle les destinataires de données sont soumis leur impose des obligations qui vont au-delà des restrictions strictement nécessaires, adéquates et proportionnées dans une société démocratique et qui risquent d'avoir un effet contraire sur les garanties fournies par la législation applicable en matière de protection des données et les clauses contractuelles types, ou parce que la poursuite du transfert entraînerait un risque de dommages graves pour les personnes dont les données sont traitées;

49. invite le groupe de travail "Article 29" à publier des lignes directrices et des recommandations sur les garanties et les protections que doivent contenir les instruments contractuels en ce qui concerne les transferts internationaux de données européennes à caractère personnel en vue d'assurer la protection de la vie privée, ainsi que des droits et libertés fondamentaux des individus, en tenant notamment compte de la législation des pays tiers en matière de renseignement et de sécurité nationale et de la participation des entreprises qui reçoivent les données dans un pays tiers à des activités de surveillance de masse par les agences de renseignement d'un pays tiers;

50. invite la Commission à examiner sans plus attendre les clauses contractuelles types qu'elle a établies en vue de déterminer si elles assurent la protection nécessaire en ce qui concerne l'accès aux données à caractère personnel transférées en vertu des clauses à des fins de renseignement et, le cas échéant, à les revoir;

Transferts fondés sur l'accord en matière d'entraide judiciaire

51. invite la Commission à effectuer avant fin 2014 une évaluation approfondie de l'accord en matière d'entraide judiciaire existant, conformément à l'article 17 dudit accord, afin de contrôler sa mise en œuvre concrète et, plus particulièrement, de vérifier si les États-Unis l'ont bien utilisé pour obtenir des informations ou des données dans l'Union européenne et si l'accord a été contourné pour obtenir des informations directement dans l'Union européenne, ainsi que d'évaluer les incidences sur les droits fondamentaux des personnes; signale que cette évaluation doit non seulement porter sur les déclarations officielles des États-Unis pour constituer une base d'analyse suffisante, mais qu'elle doit aussi s'appuyer sur des évaluations spécifiques dans l'Union européenne; souligne que ce réexamen approfondi doit également porter sur les conséquences de l'application de l'architecture constitutionnelle de l'Union à cet instrument afin de l'adapter à la législation de l'Union, en tenant compte, notamment, du protocole 36 et de l'article 10 de ladite législation et de la déclaration 50 concernant ce protocole; demande également au Conseil et à la Commission d'évaluer les accords bilatéraux entre les États membres

et les États-Unis afin de veiller à ce qu'ils soient en adéquation avec ceux que l'Union a mis ou décide de mettre en place avec les États-Unis;

Entraide judiciaire européenne en matière pénale

52. invite le Conseil et la Commission à informer le Parlement au sujet de l'utilisation effective par les États membres de la convention relative à l'entraide judiciaire en matière pénale entre les États membres, et notamment du titre III relatif à l'interception des télécommunications; invite la Commission à présenter une proposition, conformément à la déclaration 50, concernant le protocole 36, comme demandé, avant fin 2014 en vue de l'adapter au cadre du traité de Lisbonne;

Transferts basés sur les accords TFTP et PNR

53. estime que les informations fournies par la Commission européenne et le département du Trésor des États-Unis ne précisent pas si les agences de renseignement américaines ont accès aux messages financiers SWIFT dans l'Union européenne en interceptant les réseaux SWIFT ou les systèmes d'exploitation ou les réseaux de communication des banques, seules ou en coopération avec des agences de renseignement nationales européennes et sans avoir recours aux canaux bilatéraux existants en matière d'entraide judiciaire et de coopération judiciaire,

54. réaffirme sa résolution du 23 octobre 2013 et invite la Commission à suspendre l'accord TFTP;

55. invite la Commission à réagir au fait que trois des principaux systèmes informatisés de réservation utilisés par les compagnies aériennes partout dans le monde sont basés aux États-Unis et que les données PNR sont sauvegardées dans des systèmes en nuage opérant sur le sol américain et régis par le droit américain, ce qui n'est pas conforme aux dispositions en matière de pertinence de la protection des données;

Accord-cadre pour la protection des données dans le domaine de la coopération policière et judiciaire ("l'accord-cadre")

56. considère qu'une solution satisfaisante au titre de l'accord-cadre en question est une condition préalable nécessaire à la pleine restauration de la confiance entre les partenaires transatlantiques;

57. demande une reprise immédiate des négociations avec les États-Unis sur l'accord-cadre, en vue de placer les droits des citoyens de l'Union européenne sur un pied d'égalité avec ceux des ressortissants des États-Unis; souligne en outre que l'accord devrait de plus permettre à tous les citoyens de l'Union d'introduire des recours administratifs et judiciaires efficaces et exécutoires aux États-Unis sans aucune discrimination;

58. invite la Commission et le Conseil à ne se lancer dans aucun autre accord ou mesure sectoriels avec les États-Unis en matière de transfert de données à caractère personnel à des fins policières tant que l'accord-cadre ne sera pas entré en vigueur;

59. exhorte la Commission à rendre compte de façon détaillée des différents points du mandat de négociation et de la situation en avril 2014 au plus tard;

Réforme dans le domaine de la protection des données

60. invite la présidence du Conseil et les États membres à accélérer leurs travaux sur l'ensemble du paquet relatif à la protection des données en vue de permettre son adoption en 2014, afin que les citoyens de l'Union puissent bénéficier d'un niveau élevé de protection des données dans un avenir très proche; souligne qu'un engagement réel et un soutien sans faille de la part du Conseil sont une condition nécessaire pour prouver la crédibilité et la fermeté de l'Union à l'égard des pays tiers;

61. souligne que le règlement relatif à la protection des données et la directive relative à la protection des données sont tous deux nécessaires pour protéger les droits fondamentaux des individus et qu'ils doivent dès lors être traités comme un tout à adopter simultanément afin de s'assurer que l'ensemble des activités de traitement de données dans l'Union prévoient un niveau élevé de protection en toutes circonstances; souligne qu'il n'adoptera des mesures de coopération en matière répressive que lorsque le Conseil aura entamé les négociations avec le Parlement et la Commission au sujet du paquet relatif à la protection des données;

62. rappelle que les notions de "prise en compte du respect de la vie privée dès la conception" et de "respect de la vie privée par défaut" participent au renforcement de la protection des données et devraient avoir le statut de norme pour tous les produits, services et systèmes proposés sur l'internet;

63. estime que l'amélioration de la transparence et des normes de sécurité pour les télécommunications et les communications en ligne est un principe nécessaire pour un meilleur régime de protection des données; demande dès lors à la Commission de présenter une proposition législative relative à des conditions générales normalisées pour les télécommunications et les communications en ligne et de charger une autorité de contrôle de vérifier le respect de ces conditions générales;

Informatique en nuage

64. observe que les pratiques mentionnées plus haut ont eu une influence négative sur la confiance dans l'informatique en nuage et dans les fournisseurs de services d'informatique en nuage américains; souligne dès lors que le développement de services en nuage et de solutions informatiques au niveau européen est un élément essentiel pour assurer la croissance et l'emploi, ainsi que la confiance dans les services et les fournisseurs de services d'informatique en nuage et pour assurer un niveau élevé de protection des données personnelles;

65. invite tous les organismes publics dans l'Union à ne pas utiliser de services en nuage qui pourraient être soumis à une législation autre que la législation européenne;

66. réaffirme ses graves préoccupations quant à la divulgation directe obligatoire de données et d'informations à caractère personnel de citoyens de l'Union, traitées dans le cadre d'accords de services d'informatique en nuage, à des pays tiers par des fournisseurs de services d'informatique en nuage soumis au droit de pays tiers ou utilisant des serveurs de stockage situés dans des pays tiers, et quant à l'accès direct à distance aux données et aux informations à caractère personnel traitées par des forces de l'ordre et des services de renseignements de pays tiers;

67. déplore qu'un tel accès soit habituellement obtenu via l'application directe de leurs propres dispositions juridiques par les autorités de pays tiers, sans recourir aux

instruments internationaux mis en place pour la coopération juridique, tels que les accords d'entraide judiciaire ou d'autres formes de coopération judiciaire;

68. demande à la Commission et aux États membres d'accélérer les travaux relatifs au partenariat européen de l'informatique en nuage, en associant pleinement la société civile et la communauté technique, comme l'IETF (Internet Engineering Task Force), et en intégrant les aspects liés à la protection des données;

69. invite instamment la Commission, lors de la négociation d'accords internationaux concernant le traitement de données à caractère personnel, à accorder une attention particulière aux risques et aux défis que l'informatique en nuage comporte pour les droits fondamentaux, et en particulier – sans s'y limiter toutefois – pour le droit à la vie privée et à la protection des données à caractère personnel, consacrés par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne; invite en outre instamment la Commission à prendre acte des dispositions nationales des partenaires de négociation régissant l'accès des forces de l'ordre et des services de renseignement aux données à caractère personnel traitées par des services d'informatique en nuage, en particulier en exigeant que l'accès ne puisse être accordé qu'au terme d'une procédure régulière fondée sur une base juridique sans ambiguïté, et qu'à condition qu'il soit exigé de spécifier les conditions exactes d'accès, la finalité de cet accès, les mesures de sécurité mises en place lors du transfert des données, les droits des particuliers, ainsi que les règles relatives à la surveillance et à un mécanisme de recours efficace;

70. rappelle que toutes les entreprises fournissant des services dans l'Union doivent, sans exception, se conformer au droit de l'Union et qu'elles sont responsables de tout manquement et souligne qu'il importe de disposer de sanctions administratives effectives, proportionnées et dissuasives à l'encontre des fournisseurs de services d'informatique en nuage qui ne respectent pas les normes de l'Union en matière de protection des données;

71. demande à la Commission et aux autorités compétentes des États membres d'évaluer dans quelle mesure les règles européennes en matière de vie privée et de protection des données ont été enfreintes grâce à la coopération d'entités juridiques de l'Union européenne avec les services secrets ou l'acceptation de mandats délivrés par un tribunal d'un pays tiers pour demander des données à caractère personnel de citoyens de l'Union, à l'encontre de la législation européenne en matière de protection des données;

72. demande aux entreprises fournissant de nouveaux services utilisant des "données massives" et de nouvelles applications, telles que l'"internet des objets", d'intégrer dès la phase de développement des mesures de protection des données de manière à maintenir un degré élevé de confiance chez les citoyens;

Partenariat transatlantique de commerce et d'investissement (TTIP)

73. reconnaît que l'Union européenne et les États-Unis poursuivent les négociations relatives à un partenariat transatlantique de commerce et d'investissement, qui revêt une importance stratégique majeure pour la croissance économique;

74. souligne avec force, compte tenu de l'importance de l'économie numérique dans la relation et dans la cause du rétablissement de la confiance entre l'Union européenne et les États-Unis, que l'approbation du TTIP final par le Parlement européen pourrait être

menacée tant que les activités de surveillance de masse aveugle et l'interception des communications au sein des institutions et des représentations diplomatiques de l'Union européenne n'auront pas été complètement abandonnées et qu'une solution adéquate n'aura pas été trouvée en ce qui concerne les droits des citoyens de l'Union européenne en matière de confidentialité des données, notamment un recours administratif et un recours judiciaire; souligne que le Parlement européen ne peut approuver le TTIP final qu'à condition que l'accord respecte pleinement, entre autres, les droits fondamentaux reconnus par la charte de l'Union européenne, et que la protection de la vie privée des individus en ce qui concerne le traitement et la diffusion des données à caractère personnel doit continuer à être régie par l'article XIV de l'AGCS; souligne que la législation européenne en matière de protection des données ne saurait être vue comme une "discrimination arbitraire ou injustifiable" au sens de l'article XIV de l'AGCS;

Contrôle démocratique des services de renseignement

75. souligne que, bien que le contrôle des activités des services de renseignement doive s'appuyer à la fois sur la légitimité démocratique (cadre juridique solide, autorisation ex ante et vérification ex post), et sur une capacité et une expertise techniques suffisantes, ces deux aspects, et en particulier les capacités techniques, font cruellement défaut dans la majorité des organes de contrôle européens et américains actuels;

76. invite, comme il l'a fait dans le cas d'ECHELON, l'ensemble des parlements nationaux qui ne l'ont pas encore fait à mettre en place une surveillance appropriée des activités de renseignement assurée par les parlementaires ou des organes spécialisés juridiquement habilités à enquêter; invite les parlements nationaux à s'assurer que ces comités/organes de surveillance disposent des ressources, de l'expertise technique et des moyens juridiques, notamment le droit d'effectuer des visites sur place, nécessaires pour pouvoir contrôler efficacement les services de renseignement;

77. demande la création d'un groupe de députés et d'experts qui examinerait, de manière transparente et en collaboration avec les parlements nationaux, des recommandations pour améliorer le contrôle démocratique, y compris le contrôle parlementaire, des services de renseignement et pour renforcer la collaboration dans l'Union en matière de contrôle, en particulier en ce qui concerne la dimension transfrontière de cette collaboration; invite ce groupe à envisager la possibilité de définir des normes ou des règles minimales contraignantes à l'échelle de l'Europe sur le contrôle (ex ante et ex post) des services de renseignement, fondées sur les bonnes pratiques existantes et sur les recommandations d'organisations internationales (les Nations unies, le Conseil de l'Europe, etc.); y compris sur la question des organes de contrôle considérés comme un tiers au titre de la règle du "tiers service", ou sur le principe du "contrôle par l'entité d'origine", sur le contrôle et la responsabilité des services de renseignement de pays étrangers des critères de transparence renforcée, fondés sur le principe général d'accès à l'information et sur les principes dits "de Tshwane"[87], ainsi que les principes concernant les limites de la durée et de la portée de la surveillance, en veillant à ce qu'elles soient proportionnées et limitées à leur objectif;

78. demande à ce groupe de préparer un rapport et de collaborer à l'organisation d'une conférence à l'initiative du Parlement avec les organes de contrôle nationaux, qu'ils soient parlementaires ou indépendants, avant le début de l'année 2015;

---

87 "The Global Principles on National Security and the Right to Information", juin 2013.

79. invite les États membres à s'appuyer sur les bonnes pratiques en vue de permettre à leurs organes de contrôle d'accéder plus facilement aux informations sur les activités de renseignement (informations classées secrètes et informations d'autres services comprises) et de leur conférer le pouvoir d'effectuer des visites sur place, de les doter d'un ensemble solide de compétences en matière d'interrogation, de même que de l'expertise technique suffisante et des ressources nécessaires, de bénéficier d'une stricte indépendance vis-à-vis du pouvoir exécutif et de les obliger à rendre compte de la situation auprès de leurs parlements respectifs;

80. invite les États membres à développer la coopération entre les organes de contrôle, notamment au sein du réseau européen des organes nationaux de contrôle des services de renseignement (ENNIR);

81. invite instamment la VP/HR à rendre régulièrement compte des activités du centre d'analyse du renseignement de l'Union (IntCen), qui fait partie du Service européen pour l'action extérieure, aux organes compétents du Parlement, y compris sur son respect plein et entier des droits fondamentaux et des règles de l'Union applicables en matière de confidentialité des données, de façon à permettre au Parlement d'exercer un meilleur contrôle sur la dimension extérieure des politiques de l'Union; invite instamment la Commission et la VP/HR à présenter une proposition de base juridique pour les activités de l'IntCen, dans l'éventualité où seraient envisagées des opérations ou compétences futures en matière de dispositifs de renseignement ou de collecte de données qui lui soient propres pouvant avoir une incidence sur la stratégie de sécurité intérieure de l'Union;

82. invite la Commission à présenter, avant décembre 2014, une proposition concernant une procédure européenne d'habilitation de sécurité pour l'ensemble des titulaires européens d'une charge publique, étant donné que le système actuel, qui s'appuie sur l'habilitation de sécurité réalisée par l'État membre dont la personne est ressortissante, prévoit des conditions différentes et des procédures d'une durée variable selon les systèmes nationaux, ce qui se traduit par un traitement différent des députés et de leur personnel en fonction de leur nationalité;

83. rappelle les dispositions de l'accord interinstitutionnel entre le Parlement européen et le Conseil relatif à la transmission au Parlement et au traitement par celui-ci des informations classées secrètes, détenues par le Conseil concernant des questions autres que celles relevant de la politique étrangère et de sécurité commune, qui doivent servir à améliorer le contrôle au niveau de l'Union;

Agences de l'Union européenne

84. invite l'autorité de contrôle commune d'Europol, de même que les autorités nationales responsables de la protection des données, à réaliser une inspection conjointe avant la fin 2014 en vue de vérifier si les informations et les données à caractère personnel communiquées à Europol ont été obtenues légalement par les autorités nationales, et notamment si les informations ou les données ont d'abord été obtenues par des services de renseignement dans l'Union ou dans un pays tiers, et si des mesures appropriées sont en place pour prévenir l'utilisation et la diffusion ultérieure de ces informations ou de ces données; estime qu'Europol ne devrait pas traiter les informations et les données obtenues en violation des droits fondamentaux protégés par la charte des droits fondamentaux;

85. invite Europol à se prévaloir pleinement de son mandat pour demander aux autorités compétentes des États membres à lancer des enquêtes criminelles au sujet des cyberattaques majeures et des atteintes informatiques ayant un impact transfrontalier potentiel; est convaincu que le mandat d'Europol devrait être renforcé pour lui permettre de lancer sa propre enquête à la suite d'une suspicion d'attaque malveillante sur le réseau et les systèmes informatiques de deux États membres ou organes de l'Union ou davantage[88]; demande à la Commission de passer en revue les activités du centre européen de lutte contre la cybercriminalité (EC3) et de présenter, le cas échéant, une proposition de cadre général visant au renforcement des compétences de ce dernier;

Liberté d'expression

86. se déclare profondément préoccupé par les atteintes de plus en plus nombreuses à la liberté de la presse et par l'effet paralysant qu'ont sur les journalistes les intimidations des autorités nationales, notamment en ce qui concerne la protection de la confidentialité des sources journalistiques; réitère l'appel lancé dans sa résolution du 21 mai 2013 sur "la Charte de l'UE: ensemble de normes pour la liberté des médias à travers l'UE";

87. prend acte de la détention de David Miranda et de la saisie du matériel en sa possession par les autorités du Royaume-Uni en vertu de l'annexe 7 à la loi sur le terrorisme de 2000 (*Terrorism Act*) (ainsi que la demande adressée au journal *The Guardian* de détruire ou de remettre le matériel), et fait part de ses préoccupations au vu de ce que ceci constitue une potentielle grave atteinte au droit à la liberté d'expression et à la liberté des médias, reconnue par l'article 10 de la CEDH et l'article 11 de la charte de l'Union européenne, et que la législation visant à lutter contre le terrorisme pourrait faire l'objet d'abus dans de tels cas;

88. attire l'attention sur la situation difficile des lanceurs d'alerte et de leurs soutiens, y compris des journalistes, à la suite de leurs révélations; invite la Commission à examiner si une future proposition législative établissant un programme européen efficace et global de protection des lanceurs d'alerte, tel que l'a déjà demandé le Parlement dans sa résolution du 23 octobre 2013, devrait inclure également d'autres domaines de la compétence de l'Union, avec une attention toute particulière portée à la complexité du lancement d'alertes dans le domaine du renseignement; demande aux États membres d'examiner de manière approfondie la possibilité d'octroyer aux lanceurs d'alerte une protection internationale contre les poursuites;

89. demande aux États membres de faire en sorte que leur législation, notamment dans le domaine de la sécurité nationale, prévoie une alternative sûre au silence pour divulguer ou signaler les actes répréhensibles, y compris la corruption, les infractions pénales, les violations d'obligations juridiques, les erreurs judiciaires et les abus d'autorité, ce qui est également conforme aux dispositions des différents instruments internationaux (Nations unies et Conseil de l'Europe) de lutte contre la corruption, aux principes établis dans la résolution de l'Assemblée parlementaire du Conseil de l'Europe 1729 (2010), les principes de Tshwane, etc.;

Sécurité informatique dans l'Union européenne

---

[88] Position du Parlement européen du 25 février 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) (Textes adoptés de cette date, P7_TA(2014)0121).

90. indique que les incidents récents font clairement ressortir l'extrême vulnérabilité de l'Union européenne, et plus particulièrement des institutions de l'Union, des gouvernements et des parlements nationaux, des grandes entreprises européennes et des infrastructures et des réseaux informatiques européens, aux attaques sophistiquées réalisées au moyen de logiciels complexes et malveillants; observe que ces attaques exigent de tels moyens financiers et humains qu'elles émanent probablement d'entités étatiques agissant pour le compte de gouvernements étrangers; dans ce contexte, considère l'affaire du piratage ou de l'espionnage de la société de télécommunications Belgacom comme un exemple inquiétant d'attaque contre la capacité informatique de l'Union; souligne que le renforcement de la capacité et de la sécurité informatiques de l'Union atténue également la vulnérabilité de l'Union par rapport aux graves cyberattaques provenant de grandes organisations criminelles ou de groupes terroristes;

91. estime que les révélations en matière de surveillance de masse qui ont provoqué cette crise peuvent être l'occasion pour l'Europe de prendre l'initiative pour mettre en place, en tant que mesure stratégique prioritaire, une capacité autonome de ressources informatiques clés; souligne que pour regagner la confiance, une telle capacité informatique européenne devrait se fonder autant que possible sur des normes ouvertes, des logiciels et, si possible, du matériel ouverts, rendant toute la chaîne d'approvisionnement transparente et contrôlable, de l'architecture de processeur jusqu'à la couche application; fait observer que pour regagner en compétitivité dans le secteur stratégique des services informatiques, il convient de mettre en place un "*new deal* numérique" accompagné d'efforts conjoints et à grande échelle dans l'Union européenne de la part des institutions, des États membres, des instituts de recherche, de l'industrie et de la société civile; invite la Commission et les États membres à profiter des marchés publics pour promouvoir cette capacité dans l'Union en faisant des normes de sécurité et de respect de la vie privée dans l'Union une condition essentielle dans les marchés publics de produits et de services informatiques; exhorte par conséquent la Commission à réexaminer les pratiques actuelles de passation de marchés publics eu égard au traitement des données afin d'envisager de limiter les procédures d'appels d'offres aux entreprises certifiées, et éventuellement aux entreprises de l'Union européenne, lorsque des questions de sécurité ou autres intérêts vitaux sont en jeu;

92. condamne vivement le fait que des services de renseignement cherchent à assouplir les normes de sécurité informatique et à installer des "portes dérobées" ("backdoors") dans toute une série de systèmes informatiques; demande à la Commission de présenter une proposition législative visant à interdire le recours aux portes dérobées par les services répressifs; recommande en conséquence le recours aux logiciels ouverts à chaque fois que la sécurité informatique est un enjeu important;

93. invite l'ensemble des États membres, la Commission, le Conseil et le Conseil européen à soutenir sans réserve, y compris au moyen de financements dans le domaine de la recherche et du développement, le développement des capacités innovatrices et technologiques européennes en matière d'outils, de sociétés et de fournisseurs dans le secteur de l'informatique (matériel, logiciels, services et réseau), notamment aux fins de la cybersécurité et des capacités de cryptage et cryptographiques; invite toutes les institutions compétentes de l'Union et les États membres à investir dans des technologies indépendantes et locales européennes, et à développer massivement et à renforcer les capacités de détection;

94. invite la Commission, les organes de normalisation et l'ENISA à définir, avant décembre 2014, des normes et des règles minimales de sécurité et de respect de la vie privée pour les systèmes, les réseaux et les services informatiques, y compris les services d'informatique en nuage, afin de mieux protéger les données à caractère personnel des citoyens de l'Union et l'intégrité de tous les systèmes informatiques; estime que ces normes pourraient devenir la référence en vue de nouvelles normes mondiales et devraient être définies dans le cadre d'un processus ouvert et démocratique, qui ne soit pas dirigé par un pays, une entité ou une société multinationale uniques; est d'avis que, bien que des questions légitimes de maintien de l'ordre et de renseignement doivent être prises en considération afin de faciliter la lutte contre le terrorisme, ces préoccupations ne doivent pas déboucher sur un affaiblissement généralisé de la fiabilité de l'ensemble des systèmes informatiques; soutient les récentes décisions de l'IETF (Internet Engineering Task Force) visant à inclure les gouvernements dans le modèle de menace pour la sécurité de l'internet;

95. indique que les régulateurs des télécommunications européens et nationaux, et dans certains cas les sociétés de télécommunications également, ont clairement négligé la sécurité informatique de leurs utilisateurs et de leurs clients; invite la Commission à utiliser pleinement les compétences qui lui sont conférées en vertu de la directive-cadre sur la vie privée et les communications électroniques pour renforcer la protection de la confidentialité des communications en adoptant des mesures visant à s'assurer que l'équipement terminal est compatible avec le droit des utilisateurs de contrôler et de protéger leurs données à caractère personnel, et pour assurer un niveau de sécurité élevé des réseaux et services de télécommunication, notamment en imposant un cryptage de pointe de bout en bout des communications;

96. est favorable à la stratégie de cybersécurité de l'Union, mais considère qu'elle n'aborde pas toutes les menaces possibles et qu'elle devrait être étendue aux comportements malveillants des États; souligne la nécessité de renforcer la sécurité et la résilience des systèmes informatiques;

97. invite la Commission à présenter, en janvier 2015 au plus tard, un plan d'action en vue de renforcer l'indépendance de l'Union européenne dans le secteur informatique, prévoyant une approche plus cohérente afin de renforcer les capacités technologiques informatiques européennes (systèmes, équipement, services informatiques, informatique en nuage, cryptage et anonymisation) et de protéger l'infrastructure informatique critique (y compris en termes de propriété et de vulnérabilité);

98. invite la Commission à affecter, dans le cadre du prochain programme de travail du programme Horizon 2020, des moyens supplémentaires à la promotion de la recherche, du développement, de l'innovation et de la formation européens dans le domaine des technologies informatiques, et notamment des technologies et des infrastructures visant à renforcer la protection de la vie privée, de la cryptologie, de l'informatique sécurisée, les meilleures solutions de sécurité possibles, y compris les solutions de sécurité ouvertes, et d'autres services de la société de l'information, et à promouvoir également le marché intérieur des logiciels et matériels européens et des moyens et infrastructures de communication cryptés, y compris en développant une stratégie industrielle globale de l'Union européenne dans le domaine de l'industrie informatique; estime que les petites et moyennes entreprises jouent un rôle particulier dans la recherche; souligne qu'aucun financement de l'Union ne devrait être accordé aux projets dont l'unique objectif est de développer des outils permettant d'accéder illégalement à des systèmes informatiques;

99. invite la Commission à établir les responsabilités actuelles et à examiner, avant décembre 2014, la nécessité d'un mandat élargi, d'une meilleure coordination et/ou de ressources et de capacités techniques supplémentaires pour l'ENISA, le centre de lutte contre la cybercriminalité d'Europol et d'autres centres de l'Union disposant d'expertises spécialisées, la CERT-EU et le CEPD afin de leur permettre de jouer un rôle essentiel dans la sécurisation des systèmes européens de communication, de prévenir et d'enquêter plus efficacement sur les atteintes informatiques majeures dans l'Union et de réaliser (ou d'aider les États membres et les organes de l'Union à réaliser) plus efficacement les enquêtes techniques sur place liées à des atteintes informatiques majeures; invite en particulier la Commission à envisager de renforcer le rôle de l'ENISA de défense des systèmes internes au sein des institutions de l'Union et à établir au sein de la structure de l'ENISA une équipe d'intervention en cas d'urgence informatique (CERT) pour l'Union européenne et ses États membres;

100. demande à la Commission d'évaluer la nécessité d'une académie informatique européenne, qui rassemblerait les meilleurs experts européens et internationaux indépendants dans tous les domaines connexes et qui serait chargée d'offrir à l'ensemble des institutions et des organes pertinents de l'Union des conseils scientifiques sur les technologies informatiques, y compris les stratégies liées à la sécurité;

101. invite les services compétents du secrétariat du Parlement européen, sous la responsabilité du Président du Parlement, à effectuer, avant juin 2015, avec un rapport intermédiaire avant décembre 2014, un examen et une évaluation complets de la fiabilité du Parlement sur le plan de la sécurité informatique, en s'intéressant plus particulièrement aux moyens budgétaires, aux ressources en personnel, aux capacités techniques, à l'organisation interne et à l'ensemble des éléments pertinents, en vue d'améliorer la sécurité des systèmes informatiques du Parlement; considère que cette évaluation doit au moins produire des informations, des analyses et des recommandations sur:

- la nécessité de réaliser des audits réguliers, rigoureux et indépendants sur la sécurité et des essais de pénétration, en sélectionnant des experts en sécurité externes qui assurent la transparence et garantissent des références vis-à-vis de pays tiers ou de tout type de groupe d'intérêts;

- l'inclusion dans les procédures d'appels d'offres relatives aux nouveaux systèmes informatiques de conditions spécifiques en matière de sécurité informatique et de respect de la vie privée s'appuyant sur les meilleures pratiques, y compris la possibilité d'une condition relative à des logiciels ouverts ("open source") en tant que condition d'achat, ou de la condition pour les entreprises européennes de participer aux appels d'offres lorsque ceux-ci concernent des domaines sensibles liés à la sécurité;

- la liste des sociétés sous contrat avec le Parlement européen dans les domaines de l'informatique et des télécommunications, en prenant en considération toute information révélée au sujet de leur coopération avec des agences de renseignement (telles que les révélations à propos des contrats conclus par la NSA avec des entreprises telles que RSA, dont les produits sont utilisés par le Parlement européen en vue de protéger l'accès à distance à ses données par ses députés et son personnel), y compris la faisabilité que ces mêmes services soient fournis par d'autres entreprises, de préférence européennes;

– la fiabilité et la résilience des logiciels, et en particulier des logiciels commerciaux prêts à l'emploi, utilisés par les institutions de l'Union dans leurs systèmes informatiques en ce qui concerne les pénétrations et les intrusions par les autorités policières et de renseignement européennes et non européennes, compte tenu également des normes internationales applicables, des principes de gestion des risques pour la sécurité conformément aux meilleures pratiques et du respect des normes de sécurité des informations des réseaux de l'Union européenne en matière de violations de la sécurité;

– le recours accru aux systèmes ouverts;

– les démarches et mesures à prendre pour faire face au recours accru aux outils mobiles (comme les smartphones, les tablettes, qu'ils soient professionnels ou personnels) et à ses conséquences sur la sécurité informatique du système;

– la sécurité des communications entre différents lieux de travail du Parlement et des systèmes informatiques utilisés au Parlement;

– l'utilisation et l'emplacement des serveurs et des centres informatiques pour les systèmes informatiques du Parlement et les conséquences pour la sécurité et l'intégrité des systèmes;

– la mise en œuvre concrète de la réglementation existante sur les atteintes à la sécurité et la notification rapide des autorités compétentes par les fournisseurs de réseaux de télécommunication accessibles au public;

– l'utilisation de services d'informatique et de stockage en nuage par le Parlement, y compris la nature des données stockées en nuage, la manière dont le contenu et l'accès à celui-ci sont protégés et le lieu où les serveurs de nuages sont situés, en précisant le régime juridique applicable en matière de protection des données et de renseignement, ainsi qu'en évaluant les possibilités d'utiliser uniquement les serveurs de nuages basés sur le territoire de l'Union;

– un plan permettant l'utilisation de technologies cryptographiques supplémentaires, notamment le cryptage authentifié de bout en bout pour l'ensemble des services informatiques et de communication, comme l'informatique en nuage, la messagerie électronique, la messagerie instantanée et la téléphonie;

– l'utilisation des signatures électroniques dans les courriers électroniques;

– un plan pour l'utilisation d'une norme de cryptage par défaut pour les courriers électroniques, comme le GNU Privacy Guard, qui permettrait en même temps d'utiliser les signatures numériques;

– la possibilité de mettre en place un service de messagerie instantanée sécurisé au sein du Parlement, permettant une communication sécurisée, où le serveur ne verrait que du contenu crypté;

102. invite les institutions et les agences de l'Union européenne à réaliser une démarche similaire en coopération avec l'ENISA, Europol et les CERT, avant juin 2015, avec un rapport intermédiaire avant décembre 2014, notamment le Conseil européen, le Conseil,

le Service européen pour l'action extérieure (SEAE) (y compris les délégations de l'Union), la Commission, la Cour de justice de l'Union européenne et la Banque centrale européenne; invite les États membres à effectuer des évaluations similaires;

103. souligne qu'en ce qui concerne l'action extérieure de l'Union européenne, des évaluations des besoins budgétaires connexes s'imposent et des mesures initiales doivent être prises au plus vite dans le cas du Service européen pour l'action extérieure et que des moyens suffisants doivent être réservés dans le projet de budget 2015;

104. est d'avis que les systèmes informatiques à grande échelle utilisés dans le domaine de la liberté, de la sécurité et de la justice, comme le système d'information Schengen II, le système d'information sur les visas, Eurodac et les éventuels systèmes futurs tels qu'un ESTA de l'Union, doivent être développés et exploités de sorte à éviter que les données ne soient compromises à la suite des demandes émises par des autorités de pays tiers; invite l'eu-LISA à rendre compte au Parlement de la fiabilité des systèmes en place avant fin 2014;

105. invite la Commission et le SEAE à prendre des mesures au niveau international, avec les Nations unies notamment, et, en collaboration avec les partenaires intéressés, à mettre en œuvre une stratégie européenne en faveur de la gouvernance démocratique de l'internet en vue de prévenir l'influence injustifiée de toute entité individuelle, de toute entreprise ou de tout pays sur les activités de l'ICANN et de l'IANA en assurant une représentation appropriée de l'ensemble des parties concernées au sein de ces organes, tout en évitant de faciliter le contrôle ou la censure par l'État ou la "balkanisation" et la fragmentation de l'internet;

106. demande à l'Union européenne de se poser en chef de file pour façonner l'architecture et la gouvernance de l'internet afin de parer aux risques liés aux flux de données et à leur stockage, en privilégiant le renforcement de la minimisation des données et de la transparence et la réduction du stockage de masse centralisé de données brutes, et pour le réacheminement du trafic internet ou le cryptage complet de bout en bout de l'ensemble du trafic internet afin de parer aux risques actuels liés à l'acheminement inutile du trafic par le territoire de pays qui ne répondent pas aux normes de base en matière de droits fondamentaux, de protection des données et de respect de la vie privée;

107. invite à promouvoir:

- les moteurs de recherche et les réseaux sociaux de l'Union, un pas important vers l'indépendance informatique de l'Union;

- les fournisseurs de services informatiques européens;

- le cryptage des communications en général, y compris les courriels et les SMS;

- l'élaboration au niveau européen d'éléments informatiques cruciaux, par exemple les solutions pour système d'exploitation client-serveur, en utilisant les normes ouvertes et en développant des éléments européens pour le couplage de réseaux, par exemple des routeurs;

108. invite la Commission à présenter une proposition législative de système d'acheminement de l'Union, permettant notamment le traitement au niveau de l'Union des statistiques d'appel, ayant vocation à constituer une sous-structure de l'internet existant et à ne pas s'étendre au-delà des frontières de l'Union européenne; relève que toutes les données d'acheminement et statistiques d'appel devraient être traitées conformément aux cadres juridiques de l'Union;

109. invite les États membres, en collaboration avec l'ENISA, le Centre de lutte contre la cybercriminalité d'Europol, les CERT et les autorités nationales de protection des données de même que les unités nationales de lutte contre la cybercriminalité, à développer une culture de la sécurité et à lancer une campagne d'information et de sensibilisation en vue de permettre aux citoyens de faire des choix mieux informés en ce qui concerne les données à caractère personnel à mettre en ligne et le meilleur moyen de les protéger, notamment grâce au cryptage et à l'informatique en nuage sécurisée, en utilisant pleinement la plate-forme d'information sur le secteur public prévue dans la directive "Service universel";

110. invite la Commission à présenter, avant décembre 2014, des propositions législatives pour encourager les fabricants de logiciels et de matériel à renforcer la sécurité et la vie privée au moyen de fonctions dès la conception et par défaut dans leurs produits, y compris en proposant des mesures pour décourager la collecte excessive et disproportionnée de données à caractère personnel en masse et en introduisant une responsabilité légale pour les fabricants pour les vulnérabilités connues non corrigées, les produits défectueux ou non sûrs, ou l'installation de portes dérobées secrètes permettant d'accéder sans autorisation aux données et de les traiter; à cet égard, demande à la Commission d'évaluer la possibilité de mettre en place un système de certification ou de validation pour le matériel informatique, y compris des procédures de test au niveau de l'Union européenne pour garantir l'intégrité et la sécurité des produits;

Rétablissement de la confiance

111. estime, au-delà de la nécessité de modifications législatives, que l'enquête a fait ressortir la nécessité pour les États-Unis de rétablir la confiance avec leurs partenaires de l'Union, étant donné qu'il y va essentiellement des activités des agences de renseignement américaines;

112. indique que la crise de confiance qui a éclaté s'étend:

- à l'esprit de coopération au sein de l'Union européenne, certaines activités de renseignement nationales risquant de compromettre la réalisation des objectifs de l'Union;

- aux citoyens, qui se rendent compte qu'ils peuvent être espionnés non seulement par des pays tiers ou des sociétés multinationales, mais aussi par leur propre gouvernement;

- au respect des droits fondamentaux, de la démocratie et de l'état de droit, ainsi qu'à la crédibilité des garanties et du contrôle démocratiques, judiciaires et parlementaires, dans une société numérique;

Entre l'Union européenne et les États-Unis

113. rappelle l'important partenariat historique et stratégique entre les États membres de l'Union et les États-Unis, fondé sur une croyance commune dans la démocratie, l'état de droit et les droits fondamentaux;

114. estime que les activités de surveillance de masse des citoyens et d'espionnage des dirigeants politiques menées par les États-Unis ont gravement nui aux relations entre l'Union européenne et les États-Unis et eu des conséquences négatives sur la confiance dans les organisations américaines agissant dans l'Union européenne; signale que ce phénomène est encore exacerbé par l'absence de moyens de recours judiciaire ou administratif dans le cadre du droit américain pour les citoyens de l'Union, notamment dans les cas liés à des activités de surveillance à des fins de renseignement;

115. reconnaît, à la lumière des défis mondiaux auxquels sont confrontés l'Union européenne et les États-Unis, que le partenariat transatlantique doit être renforcé et qu'il est essentiel que la coopération transatlantique se poursuive dans la lutte contre le terrorisme sur une nouvelle base de confiance s'appuyant sur un véritable respect commun de l'état de droit et le rejet de toutes les pratiques de surveillance de masse systématique; affirme par conséquent que des mesures claires doivent être prises par les États-Unis pour rétablir la confiance et souligner à nouveau les valeurs fondamentales communes sur lesquelles s'appuie le partenariat;

116. est disposé à engager le dialogue avec ses homologues américains afin que, dans le débat public et au Congrès en cours aux États-Unis sur la réforme de la surveillance et le réexamen de la surveillance du renseignement, le droit à la vie privée et autres droits des citoyens et des résidents de l'Union et des autres personnes protégées par le droit de l'Union, ainsi que les droits à l'information et au respect de la vie privée équivalents dans les tribunaux des États-Unis soient garantis au moyen, par exemple, d'une révision du *Privacy Act* et de l'*Electronic Communications Privacy Act* et de la ratification du premier protocole additionnel du Pacte international relatif aux droits civils et politiques (PIDCP), de façon à mettre un terme à la discrimination actuelle;

117. demande instamment que les réformes nécessaires soient réalisées et que des garanties efficaces soient accordées aux Européens afin de veiller à ce que le recours à la surveillance et au traitement des données à des fins de renseignement étranger soit proportionné et limité à des situations bien définies et lié à des soupçons raisonnables ou à une cause probable d'activité terroriste; souligne que ces activités doivent, dans ce cas, faire l'objet d'un contrôle judiciaire transparent;

118. estime que des signaux politiques clairs s'imposent de la part de nos partenaires américains afin de démontrer que les États-Unis font la distinction entre leurs alliés et leurs adversaires;

119. exhorte la Commission européenne et le gouvernement américain à aborder, dans le cadre des négociations en cours sur l'accord-cadre entre l'Union et les États-Unis relatif au transfert de données à des fins policières, les droits à l'information et au recours judiciaire des citoyens de l'Union et à conclure ces négociations, avant l'été 2014, conformément aux engagements pris à l'occasion de la réunion ministérielle UE-États-Unis sur la justice et les affaires intérieures du 18 novembre 2013;

120. encourage les États-Unis à adhérer à la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention n° 108)

du Conseil de l'Europe, comme ils ont adhéré à la convention de 2001 sur la cybercriminalité, renforçant ainsi le fondement juridique commun entre les alliés transatlantiques;

121. invite les institutions de l'Union à étudier les possibilités de mettre en place avec les États-Unis un code de conduite qui garantirait qu'aucune activité d'espionnage n'est réalisée à l'encontre d'institutions et d'installations européennes;

Au sein de l'Union européenne

122. estime également que la participation et les activités des États membres de l'Union européenne ont produit une perte de confiance, y compris entre États membres ainsi qu'entre les citoyens et leurs autorités nationales; est d'avis que seule une clarté totale sur les fins et les moyens de la surveillance, un débat public et, au final, une révision de la législation, y compris l'arrêt des activités de surveillance de masse et le renforcement du système de contrôle judiciaire et parlementaire, pourront rétablir la confiance perdue; rappelle les difficultés que présente l'élaboration de politiques globales de sécurité de l'Union lorsque de telles activités de surveillance de masse sont pratiquées, et souligne que le principe européen de sincère coopération requiert que les États membres s'abstiennent de mener des activités de renseignement sur le territoire d'autres États membres;

123. observe que certains États membres de l'Union s'efforcent d'assurer une communication bilatérale avec les autorités américaines à propos des allégations d'espionnage et que certains d'entre eux ont conclu (Royaume-Uni) ou envisagent de conclure (Allemagne, France) des accords dits "de lutte contre l'espionnage"; souligne que ces États membres sont tenus de respecter pleinement les intérêts et le cadre législatif de l'Union dans son ensemble; juge ces accords bilatéraux contreproductifs et inappropriés, étant donnée la nécessité d'une approche européenne de ce problème; demande au Conseil d'informer le Parlement de l'évolution des discussions menées par les États membres au sujet d'un accord mutuel de non-espionnage pour toute l'Union;

124. estime que ces accords ne doivent pas violer les traités de l'Union, en particulier le principe de la coopération loyale (visé à l'article 4, paragraphe 3, du traité UE) ou saper les politiques de l'Union en général et, plus précisément, le marché intérieur, la concurrence loyale et le développement économique, industriel et social; décide de réexaminer tous accords de ce type eu égard à leur compatibilité avec le droit européen et se réserve le droit de faire jouer les procédures du traité dans l'hypothèse où ces accords devraient s'avérer contradictoires avec les principes de cohésion ou les principes fondamentaux de l'Union sur lesquels elle s'appuie;

125. demande aux États membres de consentir tous les efforts possibles pour favoriser une meilleure coopération afin de fournir des garanties contre l'espionnage, en coopération avec les organes et agences pertinents de l'Union européenne, en vue de la protection des citoyens et des institutions de l'Union, des entreprises européennes, de l'industrie de l'Union, des infrastructures et réseaux informatiques, ainsi que de la recherche européenne; considère que la participation active des parties concernées européennes est une condition *sine qua non* d'un bon échange d'informations; souligne que les menaces de sécurité sont devenues davantage internationales, diffuses et complexes, et qu'elles requièrent une coopération européenne renforcée; est convaincu que cette évolution devrait mieux se refléter dans les traités, et demande dès lors une révision des traités

pour renforcer la notion de coopération loyale entre les États membres et l'Union en ce qui concerne l'objectif de création d'un espace de sécurité, et de prévenir l'espionnage mutuel entre États membres au sein de l'Union;

126. estime que des structures de communication non piratables (courrier électronique et télécommunications, y compris lignes terrestres et téléphones portables) et des salles de réunion ne pouvant être placées sur écoute sont absolument nécessaires dans toutes les institutions et délégations de l'Union européenne; demande par conséquent la mise en place d'un système de courrier électronique interne crypté;

127. invite le Conseil et la Commission à approuver sans délai la proposition, adoptée par le Parlement européen le 23 mai 2012, de règlement du Parlement européen relatif aux modalités d'exercice du droit d'enquête du Parlement européen et abrogeant la décision 95/167/CE, Euratom, CECA du Parlement européen, du Conseil et de la Commission, présentée sur la base de l'article 226 du traité FUE; demande une révision du traité pour étendre ces pouvoirs d'enquête afin de couvrir, sans restrictions ni exceptions, tous les domaines de compétence ou d'activité de l'Union et d'inclure la possibilité d'interroger sous serment;

Sur le plan international

128. invite la Commission à présenter, avant janvier 2015, une stratégie européenne en faveur de la gouvernance démocratique de l'internet;

129. invite les États membres à donner suite à l'appel lancé lors de la 35^{e} conférence internationale des commissaires à la protection des données et de la vie privée afin de "promouvoir l'adoption d'un protocole additionnel à l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP). Ce protocole devrait être fondé sur les normes élaborées et avalisées par la Conférence internationale ainsi que sur les précisions formulées dans l'observation générale n° 16 de la commission des droits de l'homme relative au Pacte afin de favoriser l'établissement de normes mondiales concernant la protection des données à caractère personnel et la protection de la vie privée conformément à la primauté du droit"; invite les États membres à prévoir dans cet exercice de plaider en faveur de l'attribution, à une agence internationale des Nations unies, d'un mandat consistant en particulier à surveiller l'apparition d'instruments de surveillance et à réglementer et examiner les utilisations qui en sont faites; demande à la haute représentante/vice-présidente de la Commission et au Service européen pour l'action extérieure d'adopter des mesures proactives;

130. invite les États membres à développer une stratégie cohérente et solide au sein des Nations unies, en appuyant notamment la résolution sur "le droit à la vie privée à l'ère numérique", proposée par le Brésil et l'Allemagne, telle qu'adoptée par la troisième commission de l'Assemblée générale des Nations unies (commission des droits de l'homme) le 27 novembre 2013, et à œuvrer davantage pour la défense du droit fondamental à la vie privée et à la protection des données au niveau international tout en évitant de faciliter le contrôle ou la censure par l'État ou la fragmentation de l'internet, notamment au moyen d'une initiative en faveur d'un traité international interdisant les activités de surveillance de masse et via la création d'une agence pour en assurer le contrôle;

Plan prioritaire: un habeas corpus numérique européen - protéger les droits fondamentaux à l'ère numérique

131. décide de soumettre aux citoyens, aux institutions et aux États membres de l'Union européenne les recommandations mentionnées plus haut en guise de plan prioritaire pour la prochaine législature; invite la Commission et les autres institutions, organes, bureaux et agences de l'Union visés dans la présente résolution, conformément à l'article 265 du traité FUE, à agir selon les recommandations et demandes formulées dans la présente résolution;

132. décide de lancer un habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique fondé sur les huit actions suivantes, dont il surveillera la mise en œuvre:

– Action 1: adopter le paquet relatif à la protection des données en 2014;

– Action 2: conclure l'accord-cadre entre l'Union européenne et les États-Unis garantissant le droit fondamental des citoyens au respect de la vie privée et à la protection des données et assurant des mécanismes de recours adéquats aux citoyens européens, y compris en cas de transfert de données de l'Union européenne vers les États-Unis à des fins répressives;

– Action 3: suspendre la "sphère de sécurité" jusqu'à ce qu'une analyse complète de celle-ci soit effectuée et que ses lacunes soient corrigées en veillant à ce que le transfert de données à caractère personnel à des fins commerciales à partir de l'Union européenne vers les États-Unis ne puisse se faire qu'en respectant les normes européennes les plus strictes;

– Action 4: suspendre l'accord TFTP en attendant i) la conclusion des négociations concernant l'accord-cadre; ii) la réalisation d'une enquête approfondie sur la base d'une analyse européenne et la prise en compte de l'ensemble des préoccupations soulevées par le Parlement dans sa résolution du 23 octobre 2013;

– Action 5: évaluer tout accord, mécanisme ou échange avec les pays tiers concernant des données à caractère personnel pour s'assurer que le droit au respect de la vie privée et à la protection des données à caractère personnel n'est pas violé en raison des activités de surveillance et prendre les mesures adéquates nécessaires;

– Action 6: protéger l'état de droit et les droits fondamentaux des citoyens de l'Union (y compris contre les menaces qui pèsent sur la liberté de la presse), le droit de la population à recevoir des informations impartiales et la confidentialité professionnelle (y compris dans les relations entre l'avocat et son client), et renforcer la protection des lanceurs d'alerte;

– Action 7: développer une stratégie européenne en vue d'une plus grande indépendance informatique (un "*new deal* numérique", comprenant l'affectation de ressources adéquates au niveau national et de l'Union) pour dynamiser l'industrie informatique et permettre aux entreprises européennes d'exploiter l'avantage compétitif de l'Union en termes de protection de la vie privée;

– Action 8: faire de l'Union européenne un exemple en matière de gouvernance démocratique et neutre de l'internet;

133. invite les institutions et les États membres de l'Union à promouvoir l'habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique; s'engage à se faire le défenseur du respect des droits des citoyens de l'Union, en s'appuyant sur le calendrier ci-après pour suivre la mise en œuvre:

– avril 2014 - mars 2015: un groupe de contrôle basé sur la commission d'enquête LIBE responsable de la surveillance de nouvelles révélations éventuelles concernant les mandats d'enquête et du suivi de la mise en œuvre de la présente résolution;– à partir de juillet 2014: un mécanisme de surveillance permanent des transferts de données et des recours judiciaires au sein de la commission compétente;

– printemps 2014: une demande formelle au Conseil européen d'intégrer l'habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique dans les lignes directrices à adopter au titre de l'article 68 du traité FUE;

– automne 2014: un engagement selon lequel l'habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique et les recommandations connexes serviront de critères déterminants pour l'approbation de la prochaine Commission;

– 2014: une conférence rassemblant des experts européens de haut niveau dans différents domaines relatifs à la sécurité des technologies de l'information (y compris les mathématiques, la cryptographie, les technologies de renforcement de la protection de la vie privée, etc.) afin d'encourager la définition d'une stratégie européenne concernant les technologies de l'information pour la législature à venir;

– 2014-2015: un groupe axé sur la confiance/les données/les droits des citoyens, formé par le Parlement européen et le Congrès américain, ainsi que les parlements d'autres pays tiers engagés dans le processus, comme le Brésil, et qui se réunira régulièrement;

– 2014-2015: une conférence avec les organes de surveillance des services de renseignement des parlements nationaux européens;

o

o o

134. charge son Président de transmettre la présente résolution au Conseil européen, au Conseil, à la Commission, aux parlements et aux gouvernements des États membres, aux autorités nationales chargées de la protection des données, au CEPD, à l'eu-LISA, à l'ENISA, à l'Agence des droits fondamentaux, au groupe de travail "Article 29", au Conseil de l'Europe, au Congrès des États-Unis d'Amérique, au gouvernement

américain, au Président, au gouvernement et au parlement de la République fédérative du Brésil et au Secrétaire général des Nations unies;

135. charge sa commission des libertés civiles, de la justice et des affaires intérieures à s'adresser au Parlement en plénière sur le sujet un an après l'adoption de la présente résolution; considère qu'il est essentiel d'évaluer la mesure dans laquelle les recommandations adoptées par le Parlement ont été suivies et d'analyser tous les cas où de telles recommandations n'ont pas été suivies.