5 - 2855/1

SÉNAT DE BELGIQUE

SESSION DE 2013-2014

16 AVRIL 2014

Proposition de résolution relative aux communications de la Commission européenne visant à rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis du point de vue des citoyens et des entreprises

(Déposée par M. Benoit Hellings)

DÉVELOPPEMENTS

Le développement de l'économie numérique a entraîné une croissance exponentielle de la quantité, de la qualité, de la diversité et de la nature des activités de traitement de données.

Dans le cadre des relations transatlantiques, les données privées des citoyens, des entreprises et des institutions de l'Union européenne, intéressent les États-Unis à plus d'un titre.

Il s'agit en réalité d'un bien plus que précieux en valeur marchande : la valeur estimée des données des citoyens de l'Union européenne était de 315 milliards d'euros en 2011 et ce montant devrait approcher le billion d'euros par an d'ici à 2020 (1). C'est également un secteur prometteur en termes de développement d'analyses de grands ensembles de données (*big data*).

Toutefois, l'utilisation de ces données et les méthodes modernes de traitement des données soulèvent des questions fondamentales, exacerbées dans le cadre des révélations relatives au programme de surveillance à grande échelle PRISM, mais également dans le cadre de l'affaire SWIFT ou des échanges de données passagers

(1) Voir Boston Consulting Group, « *The Value of our Digital Identity* », novembre 2012.

BELGISCHE SENAAT

ZITTING 2013-2014

16 APRIL 2014

Voorstel van resolutie betreffende de mededelingen van de Europese Commissie tot herstel van het vertrouwen van burgers en ondernemingen in de gegevensstromen tussen de Europese Unie en de Verenigde Staten

(Ingediend door de heer Benoit Hellings)

TOELICHTING

De ontwikkeling van de digitale economie heeft de omvang, de kwaliteit, de diversiteit en de aard van gegevensverwerkingsactiviteiten exponentieel doen toenemen.

In het raam van de trans-Atlantische betrekkingen interesseren privégegevens van burgers, ondernemingen en instellingen van de Europese Unie de Verenigde Staten in meer dan een opzicht.

In feite zijn persoonsgegevens erg waardevol : de waarde van de gegevens van de EU-burgers in 2011 werd op 315 miljard euro geschat en zou tegen 2020 jaarlijks oplopen tot bijna één biljoen euro (1). Het is ook een veelbelovende sector voor de analyse van omvangrijke gegevensverzamelingen (*big data*).

Het gebruik van die gegevens en de moderne methoden voor het verwerken van gegevens roepen evenwel belangrijke vragen op die nog prangender worden door de onthullingen over het grootschalige observatieprogramma PRISM, door de zaak SWIFT en door de uitwisseling van passagiersgegevens (PNR). Elk van die

(1) Zie Boston Consulting Group, « *The Value of our Digital Identity* », november 2012.

(PNR). Un point commun : le potentiel dévastateur de ces programmes pour les droits fondamentaux des Européens en matière de protection de la vie privée, qui mettent à mal les relations entre les États-Unis et l'Union européenne.

L'optique de la Commission européenne au travers deux récentes communications au Parlement et au Conseil (1) est de tenter de reconstruire une confiance des citoyens européens dans les flux de leurs données vers les États-Unis, confiance mise à mal par les affaires précitées.

Pour l'auteur de la présente proposition, l'enjeu doit également et surtout être de garantir le respect absolu des droits européens dans le cadre de ces échanges.

I. Les instruments qui structurent les relations entre les USA et l'Union européenne en matière de transfert de données.

L'enjeu d'une recherche de confiance et de garantie du respect des droits fondamentaux des européens dans les flux de données vers les USA est à situer en considérant l'ensemble des instruments qui structurent actuellement les relations USA et l'Union européenne en matière de transfert de données.

1. Données transférées à des fins judiciaires

Il existe actuellement trois — et bientôt quatre, — accords multilatéraux auxquels la Belgique est partie prenante :

— l'Accord PNR (*Passenger Name Record*), un accord d'entraide judiciaire sur l'utilisation et le transfert des données des dossiers des passagers (2) à propos duquel la commission de l'Intérieur du Sénat a remis un avis critique, sur la base d'une proposition de résolution déposée par Ecolo et Groen (3) ;

(1) Communication de la Commission au Parlement européen et au Conseil : Rétablir la confiance dans les flux de données entre l'Union européenne et les USA — COM(2013) 846, et communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire — COM(2013) 847.

(2) Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieur.

(3) Proposition de résolution relative à la proposition de décision du Conseil européen relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la Sécurité intérieure, Doc. Sénat n° 5-1534/1-2011/2012.

programma's kan vernietigend zijn voor de grondrechten van de Europese burgers inzake de bescherming van de persoonlijke levenssfeer en bemoeilijkt de betrekkingen tussen de Verenigde Staten en de Europese Unie.

Met twee nieuwe mededelingen aan het Parlement en de Raad (1) wil de Europese Commissie het door voornoemde zaken geschonden vertrouwen van de Europese burgers in de gegevensstromen naar de Verenigde Staten herstellen.

Volgens de indiener van dit voorstel moet bij die gegevensuitwisseling vooral de eerbiediging van de Europese rechten gewaarborgd worden.

I. De instrumenten die de betrekkingen regelen tussen de VS en de Europese Unie betreffende de doorgifte van gegevens.

De zoektocht naar vertrouwen en naar het waarborgen van de grondrechten van de Europese burgers binnen de gegevensstromen naar de VS, moet worden beschouwd binnen het geheel aan instrumenten dat momenteel de betrekkingen regelt tussen de VS en de Europese Unie wat de doorgifte van gegevens betreft.

1. Doorgifte van gegevens voor gerechtelijke doeleinden

Momenteel bestaan er drie multilaterale akkoorden — binnenkort vier — waarbij België partij is :

— de PNR-Overeenkomst (*Passenger Name Record*), een overeenkomst over rechtshulp in verband met het gebruik en de doorgifte van persoonsgegevens van passagiers (2), waarover de commissie voor de Binnenlandse Zaken van de Senaat een kritisch advies uitbracht op basis van een voorstel van resolutie ingediend door Ecolo en Groen (3) ;

(1) Mededeling van de Commissie aan het Europees Parlement en de Raad : Herwinnen van vertrouwen in dataoverdrachten tussen de EU en de VS — COM(2013)846, en mededeling van de Commissie aan het Europees Parlement en de Raad betreffende de werking van de veiligehavenregeling (« *Safe Harbour* ») uit het oogpunt van EU-burgers en in de EU gevestigde ondernemingen — COM(2013) 847.

(2) Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie inzake het gebruik en de doorgifte van persoonsgegevens van passagiers aan het Amerikaanse ministerie van Binnenlandse Veiligheid.

(3) Voorstel van resolutie betreffende het voorstel voor een besluit van de Europese Raad tot sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR-gegevens) aan het Amerikaanse ministerie van Binnenlandse Veiligheid, stuk Senaat, nr. 5-1534/1-2011/2012.

— le TFTP (*Terrorist Finance Tracking Programme*), un accord sur le traitement et le transfert des données de messagerie financière aux fins du programme de surveillance du financement du terrorisme (1) ;

— l'Accord entre Europol et les USA ;

— l'Accord-cadre sur la protection des données dans le domaine de la coopération policière et judiciaire visant à assurer un niveau élevé de protection des données, actuellement négocié entre l'Union européenne est les USA et dont l'achèvement est prévu dans un délai très court (avant l'été 2014).

Avant de transmettre les communications examinées, et face aux inquiétudes suscitées dans l'Union européenne par la collecte et le traitement à grande des citoyens échelle d'informations à caractère personnel dans le cadre de programmes américains de surveillance, la Commission européenne a activé les mécanismes de révision conjointe permettant d'examiner la mise en œuvre des Accords PNR et TFTP.

— Pour l'accord PNR, le rapport de la Commission européenne (2) constate qu'une plus grande transparence est nécessaire dans le droit d'accès à leurs données sans exception, que la durée de conservation avant dépersonnalisation des données dépasse les six mois prévus dans l'accord, qu'il y a recours trop systématique à la méthode « *push* » alors qu'elle devrait être occasionnelle. Par conséquent, la Commission recommande de renouveler un examen conjoint rapidement.

— Pour l'accord TFTP, une consultation officielle a généré un engagement écrit des États-Unis assurant qu'aucune collecte directe de données n'avait lieu en violation de l'accord. La nécessité d'un tel écrit pose question, vu qu'un tel engagement est déjà contenu dans l'accord.

(1) 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 fins du programme de surveillance du financement du terrorisme.

(2) *Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security*, COM(2013) 844 final.

— het TFTP (*Terrorist Finance Tracking Programme*), een overeenkomst inzake de verwerking en doorgifte van gegevens betreffende het betalingsberichtenverkeer ten behoeve van het Programma voor het traceren van terrorismefinanciering (1) ;

— de overeenkomst tussen Europol en de VS ;

— de raamovereenkomst over de bescherming van gegevens in het kader van de politionele en justitiële samenwerking, die bedoeld is om een hoog beschermingsniveau voor gegevens te waarborgen, waarover de Europese Unie en de VS momenteel onderhandelen en die binnenkort zou worden afgewerkt (vóór de zomer van 2014).

Alvorens de onderzochte mededelingen te doen, en in het licht van de onrust die was ontstaan binnen de Europese Unie door de verzameling en verwerking op grote schaal van persoonlijke informatie in het raam van Amerikaanse observatieprogramma's, heeft de Europese Commissie de mechanismen tot gezamenlijke herziening geactiveerd, waardoor de uitvoering van de PNR- en de TFTP-Overeenkomst kon worden onderzocht.

— Wat de PNR-overeenkomst betreft, stelt het verslag van de Europese Commissie (2) vast dat er meer transparantie nodig is rond het absoluut recht van de burgers op toegang tot gegevens, dat de gegevens langer dan de in de overeenkomst bepaalde zes maanden worden bewaard vooraleer ze worden gedepersonaliseerd, dat de « *push* »-methode te stelselmatig gebruikt wordt, terwijl ze incidenteel moet worden toegepast ; bijgevolg beveelt de Commissie aan spoedig een nieuw gezamenlijk onderzoek uit te voeren.

— Wat de TFTP-overeenkomst betreft, bracht een officiële raadpleging de Verenigde Staten ertoe schriftelijk te verzekeren dat er geen rechtstreekse verzameling van gegevens heeft plaatsgevonden die in strijd met de bepalingen van de overeenkomst is. Dat een dergelijk schrijven nodig is, doet vragen rijzen, aangezien de overeenkomst reeds een dergelijk engagement omvat.

(1) Besluit 2010/412/EU van de Raad van 13 juli 2010 betreffende de sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering.

(2) *Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security*, COM(2013) 844 final.

De plus, ceci n'empêche pas la Commission d'avancer le prochain examen conjoint.

— En ce qui concerne l'accord Europol-USA, l'autorité de contrôle commune (ACC) a procédé, en novembre 2011, à un deuxième contrôle de la mise en œuvre des tâches d'Europol au titre de l'accord TFTP (1). Si la situation s'est améliorée par rapport à l'an passé, l'ACC affirme qu'il reste encore beaucoup à faire dans de nombreux domaines. Les demandes d'information doivent mieux justifier la nécessité du champ géographique choisi et les catégories de données à caractère personnel demandées.

On le voit, les rapports et réexamens ne rassurent pas même la Commission européenne, qui affirme qu'il y a lieu « de poursuivre à l'avenir un contrôle très étroit de la mise en œuvre des accords PNR et TFTP », dont un nouveau réexamen conjoint est prévu au printemps 2014.

À côté de ces instruments multilatéraux, il existe un certain nombre d'accords bilatéraux qui concernent la Belgique et avec lesquels un parallèle doit être fait. Dont l'Accord entre le Royaume de Belgique et les États-Unis d'Amérique sur le renforcement de la coopération dans la prévention et la lutte contre la criminalité grave, établi à Bruxelles le 20 septembre 2011, auquel le Sénat a donné son assentiment le 23 janvier 2014.

2. Données transférées à des fins commerciales

Il existe actuellement deux instruments multilatéraux importants pour encadrer les transferts de données personnelles dans un contexte commercial :

— la directive 95/46 qui fixe les règles applicables au transfert de données à caractère personnel des États membres vers des pays tiers dans la mesure où des « décisions constatent du caractère adéquat du niveau de protection » dans le pays tiers ;

— la décision (2) relative à la « sphère de sécurité » qui autorise le libre transfert d'informations à caractère personnel des États membres de l'Union européenne vers des entreprises établies aux USA qui se sont engagées à respecter les principes de la sphère de sécurité. Ce dis-

(1) L'ACC d'Europol contrôle pour la deuxième année la mise en œuvre de l'accord TFTP1, Déclaration publique, Bruxelles, 14 mars 2012.
(2) Décision 2000/520/CE.

Bovendien verhindert het niet dat de Commissie het volgend gezamenlijk onderzoek naar voren schuift.

— Wat de overeenkomst tussen Europol en de VS betreft, heeft het Gemeenschappelijk Controleorgaan (GCO) in november 2011 de uitvoering van de taken van Europol krachtens de TFTP-overeenkomst een tweede maal gecontroleerd (1). In vergelijking met vorig jaar is de situatie erop vooruit gegaan, maar het GCO verklaart dat er nog zeer veel voor verbetering vatbaar is. In de informatieverzoeken moeten het geselecteerde geografische gebied en de afzonderlijke gevraagde gegevenscategorieën beter worden gemotiveerd.

De verslagen en herzieningen stellen dus zelfs de Europese Commissie niet gerust, die het nodig vindt om « een zeer streng toezicht op de uitvoering van de PNR- en TFTP-overeenkomsten in de toekomst [voort te zetten] » ; in de lente van 2014 is er een nieuwe gezamenlijke herziening van die overeenkomsten gepland.

Naast die multilaterale instrumenten bestaan er enkele bilaterale akkoorden die betrekking hebben op België en waarmee een vergelijking moet worden gemaakt. Zoals de overeenkomst tussen het Koninkrijk België en de Verenigde Staten van Amerika voor de bevordering van de samenwerking bij het voorkomen en bestrijden van ernstige criminaliteit, gesloten te Brussel op 20 september 2011, waarmee de Senaat op 23 januari 2014 heeft ingestemd.

2. Doorgifte van gegevens voor commerciële doeleinden

Momenteel bestaan er twee belangrijke multilaterale instrumenten die een kader creëren voor de doorgifte van persoonsgegevens voor commerciële doeleinden :

— richtlijn 95/46, die regels bepaalt voor de doorgifte van persoonsgegevens van de lidstaten naar derde landen, in die zin dat er besluiten zijn inzake « het passend karakter van het beschermingsniveau dat het derde land biedt » ;

— het besluit (2) betreffende de « veilige haven », dat de vrije doorgifte toestaat van persoonsgegevens van de lidstaten van de Europese Unie naar ondernemingen die gevestigd zijn in de VS en die zich ertoe verbonden hebben de veilige haven-beginselen te

(1) Europol-GCO inspecteert voor het tweede jaar de uitvoering van de TFTP-Overeenkomst, Openbare verklaring, Brussel, 14 maart 2012.
(2) Besluit 2000/520/EG

positif rassemble aujourd'hui près de 3 246 entreprises américaines.

L'actuel accord relatif à la sphère de sécurité est fondé sur la reconnaissance par l'Union européenne des « principes de la sphère de sécurité » et des « questions fréquemment posées » publiés par le ministère du commerce américain. Cette reconnaissance fonde la décision de la Commission de considérer les États-Unis comme assurant un niveau adéquat de protection aux fins de transferts de données depuis l'Union européenne.

Le contexte des communications visant à rétablir la confiance laisse entendre que cette protection n'est pas suffisante. L'évaluation qu'en propose la Commission européenne le confirme.

Cette sphère de sécurité américaine repose sur l'adhésion volontaire des entreprises aux principes, sur l'auto-certification des entreprises adhérant aux principes et sur le contrôle par les autorités publiques du respect des engagements pris lors de l'auto-certification.

Or, le rapport de la Commission sur le fonctionnement de la sphère de sécurité met en évidence un certain nombre d'insuffisances. Parmi les lacunes qui affectent la transparence et l'exécution de cet accord, la Commission européenne relève les points suivants :

— l'obligation de déclaration d'adhésion : il existe un problème persistant des fausses déclarations d'adhésions qui concernerait 10 % des entreprises adhérentes ;

— l'obligation de rendre publiques leurs dispositions de protection de la vie privée : les rapports successifs montrent que le degré de respect des obligations en matière de transparence varie d'une entreprise à l'autre (jusque 10 % des entreprises pourtant certifiées n'ont pas publié ces dispositions sur leur site);

— l'obligation d'intégrer effectivement ces principes dans leur fonctionnement d'entreprise : en 2004, on constatait qu'un nombre important d'entreprises n'avaient pas correctement intégré ces principes ;

— l'absence de contrôle effectif :

• le Panel européen de la protection des données, compétent pour instruire des plaintes concernant des données recueillies dans le cadre d'une relation de

eerbiedigen. Momenteel verenigt deze bepaling bijna 3 246 Amerikaanse ondernemingen.

De huidige veilige haven-overeenkomst is gebaseerd op de erkenning door de Europese Unie van de veilige haven-beginselen en de « vaak gestelde vragen » die door het ministerie van Handel van de VS werden gepubliceerd. Het besluit van de Commissie dat de Verenigde Staten een passend beschermingsniveau bieden om de doorgifte van gegevens vanuit de Europese Unie te rechtvaardigen, berust op die erkenning.

De context waarbinnen de mededelingen worden gedaan om het vertrouwen te herstellen, geeft aan dat die bescherming niet voldoende is. De evaluatie die de Commissie ervan maakte, bevestigt dat.

Die Amerikaanse veilige haven is gebaseerd op de vrijwillige deelneming van ondernemingen, op zelfcertificering door deze deelnemende ondernemingen en op handhaving door overheidsinstanties van de uit de zelfcertificering voortvloeiende verbintenissen.

Het verslag van de Commissie over de werking van de veilige haven vestigt echter de aandacht op enkele gebreken, die afbreuk doen aan de transparantie en uitvoering van het akkoord :

— de verplichting tot aanspraak op deelneming : er is een aanhoudend probleem van valse aanspraken op deelneming ; het zou om 10 % van de deelnemende ondernemingen gaan ;

— de verplichting om hun bepalingen omtrent de bescherming van de persoonlijke levenssfeer bekend te maken : de verschillende verslagen tonen aan dat de mate waarin de verplichtingen inzake transparantie geëerbiedigd worden, verschilt van onderneming tot onderneming (tot 10 % van de nochtans gecertificeerde ondernemingen hebben die bepalingen niet bekendgemaakt op hun website);

— de verplichting om de werking van de onderneming daadwerkelijk af te stemmen op die beginselen : in 2004 werd vastgesteld dat een groot aantal ondernemingen de beginselen niet correct had toegepast ;

— de afwezigheid van effectieve handhaving :

• het Gegevensbeschermingspanel van de EU, dat bevoegd is om klachten te behandelen omtrent gegevens die werden verzameld in het raam van een werkrelatie

travail (53 % des entreprises US adhérentes) n'a traité que quatre dossiers ;

• la Commission fédérale américaine du commerce, sensée donner suite à des saisies d'autorités compétentes des États membres européens, n'a reçu aucune plainte pendant dix ans, ses sanctions prévues sont des conventions de transaction;

• le règlement extrajudiciaire des litiges (REL), soit la mise en place de mécanismes de recours pour les particuliers : certains prestataires de REL imposent des redevances aux particuliers qui décident de porter plainte (s'opposant ainsi au principe européen de gratuité);

— l'exclusion du champ de la sphère de sécurité des entreprises de télécommunications, pourtant porteuses d'un nombre important de données à caractère personnel ;

— l'absence d'obligation pour les tiers responsables de traitement que sont les sous-traitants.

En conclusion, la Commission observe qu'« en raison d'un manque de transparence et de contrôle de sa mise en œuvre, certains membres de la sphère de sécurité ayant déclaré leur adhésion à ses principes ne les respectent pas dans la pratique. Cette situation a une incidence négative sur les droits fondamentaux des citoyens de l'Union européenne. Elle désavantage aussi les entreprises européennes par rapport à leurs concurrents américains qui exercent leur activité dans le cadre de la sphère de sécurité mais qui, dans la pratique, n'observent pas ses principes. »

II. Les recommandations de la Commission européenne

Fondées sur les lacunes et violations des droits fondamentaux européens observées pour les deux ensembles d'instruments, les principales recommandations de la Commission européenne sont les suivantes :

1. Réformer les règles de l'Union européenne en matière de protection des données, dont l'aboutissement est encore officiellement prévu pour l'année 2014. Il est aujourd'hui assez vraisemblable que les discussions

(53 % van de deelnemende Amerikaanse ondernemingen), heeft slechts vier dossiers behandeld ;

• de Amerikaanse *Federal Trade Commission*, die gevolg moet geven aan klachten die worden ingediend door bevoegde overheden van Europese lidstaten, heeft in tien jaar tijd geen enkele klacht ontvangen ; de sancties waarover ze beschikt, bestaan in schikkingsovereenkomsten;

• de alternatieve geschillenbeslechting (AGB), oftewel de oprichting van verhaalmechanismen voor particulieren : bepaalde alternatieve geschillenbeslechters vragen een vergoeding van burgers die een klacht indienen (wat in strijd is met het Europese kosteloosheidsbeginsel);

— de uitsluiting van telecommunicatie-ondernemingen uit de veilige haven, hoewel zij over een zeer grote hoeveelheid persoonsgegevens beschikken ;

— de afwezigheid van een verplichting voor de derde verwerkers die de subcontractanten zijn.

Ten slotte merkt de Commissie het volgende op : « Als gevolg van een gebrek aan transparantie en handhaving neemt niet iedereen die zelf heeft verklaard de veiligehavenregeling te onderschrijven, deze beginselen in de praktijk ook in acht. Dit heeft negatieve gevolgen voor de grondrechten van de EU-burgers. Het schept ook een nadeel voor Europese ondernemingen ten opzichte van de concurrerende Amerikaanse ondernemingen die weliswaar aan de regeling deelnemen, maar de beginselen daarvan in de praktijk niet toepassen. »

II. Aanbevelingen van de Europese Commissie

Op basis van de gebreken en schendingen van de Europese grondrechten die werden vastgesteld wat de twee groepen instrumenten betreft, beveelt de Europese Commissie vooral het volgende aan :

1. Een hervorming van de EU-regels wat gegevensbescherming betreft ; officieel is de voltooiing van die hervorming nog steeds in 2014 gepland. Intussen is gebleken dat de gesprekken waarschijnlijk niet zullen zijn

n'aboutiront pas avant la fin de la législature européenne en mai 2014 (1).

Il s'agit pourtant d'une condition nécessaire puisque la réforme projetée de la protection des données à caractère personnel européenne dénote trois lacunes fondamentales présentes dans la législation actuelle : le champ d'application territorial (les entreprises qui ne sont pas établies sur le territoire européen ne sont pas tenues d'appliquer le droit de l'Union en matière de protection des données quand elles offrent des biens ou services aux consommateurs européens); l'absence de sanctions proportionnées et dissuasives et l'absence de responsabilisation et d'obligation pour les sous-traitants (par exemple *cloud*) notamment en matière de sécurité, alors qu'ils traitent un nombre de données de plus en plus important.

Il est, par ailleurs, fondamental que cette réforme s'inscrive dans l'optique de la préservation du droit à la vie privée et non dans une logique de libre circulation de ces données à caractère personnel comme cela transparait dans les propositions initiales de la Commission.

2. Rendre la sphère de sécurité plus sûre.

Toutefois, la série de souhaits formulés par la Commission ne remet pas en cause les éléments qui fondent la faiblesse du système, à savoir l'auto-certification et les dysfonctionnements majeurs dans les procédures de contrôle. La Commission se concentre sur une stratégie de « colmatage » des fuites, plutôt que sur un travail d'ensemble.

3. La négociation d'un nouvel accord-cadre sur la protection des données relatif au transfert et au traitement d'informations à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale.

Les négociations actuelles visent essentiellement la limitation des finalités, les conditions et la durée de conservation des données. Mais qu'en est-il quand on sait qu'une définition restrictive des dérogations fondées

(1) En janvier 2012, la Commission européenne a formulé une proposition de directive « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ». Son objectif était de doter l'Union européenne d'un nouveau cadre juridique relatif à la protection des données à caractère personnel. Elle a également formulé une proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (IP/12/46 25/01/2012). Néanmoins, la proposition de règlement est toujours en attente de première lecture au Parlement européen dont la date indicative n'est pas programmée avant mars 2013.

afgerond voor het einde van de Europese zittingsperiode in mei 2014 (1).

Het gaat nochtans om een noodzakelijke voorwaarde, aangezien de geplande hervorming van de Europese bescherming van persoongegevens wijst op drie fundamentele gebreken van de huidige wetgeving : het territoriale toepassingsgebied (ondernemingen die niet gevestigd zijn op het Europese grondgebied moeten het recht van de Unie betreffende gegevensbescherming niet toepassen, wanneer zij de Europese consumenten goederen of diensten aanbieden); de afwezigheid van aangepaste en ontmoedigende sancties en van verantwoordelijkheidsbesef en verplichtingen voor de subcontractanten (bijvoorbeeld *cloud*), in het bijzonder wat veiligheid betreft, terwijl zij steeds meer gegevens verwerken.

Het is overigens van fundamenteel belang dat die hervorming in de lijn ligt van het behoud van het recht op de persoonlijke levenssfeer, en niet in de lijn van een vrij verkeer van die persoonsgegevens, zoals de oorspronkelijke voorstellen van de Commissie laten uitschijnen.

2. De veilige haven veiliger maken.

Desalniettemin stellen de wensen die de Commissie formuleerde niet de zwakke punten van het systeem opnieuw ter discussie : de zelfcertificering en de belangrijkste gebreken van de controleprocedures. De Commissie richt zich vooral op « het dichten van de lekken » in plaats van het geheel aan te pakken.

3. Onderhandelingen over een nieuwe raamovereenkomst inzake de doorgifte en de verwerking van persoonsgegevens in het kader van politiële en gerechtelijke samenwerking in strafzaken.

De huidige onderhandelingen strekken er vooral toe de doelbeperking inzake de voorwaarden voor en de duur van het bewaren van gegevens te beperken. Maar een strikte definitie van de uitzonderingen om redenen

(1) In januari 2012 heeft de Europese Commissie een voorstel van richtlijn gedaan « betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens ». Het doel ervan was de Europese Unie te voorzien van een nieuw wettelijk kader voor de bescherming van persoonsgegevens. Zij heeft ook een voorstel uitgebracht voor een verordening betreffende de bescherming van fysieke personen met betrekking tot de behandeling van persoonsgegevens en het vrije verkeer van deze gegevens (IP/12/46 25/01/2012). Niettemin wacht dit voorstel van verordening nog steeds op een eerste lezing in het Europees Parlement, wat niet verwacht wordt vóór maart 2013.

sur des motifs de sécurité nationale ont déjà conduit à des programmes américains de surveillance d'une telle ampleur comme PRISM ou l'espionnage des autorités publiques européennes par la NSA ?

Il est donc très probable que les futures garanties, même si elles sont scellées dans le nouvel accord sur le cadre de la coopération entre les services répressifs, ne soient pas à la hauteur des défis posés par le comportement américain face à la législation européenne en matière de protection des données.

Par ailleurs, cette négociation ayant été ouverte en parallèle avec celle intra-européenne sur la protection des données, nous sommes donc en droit de nous interroger sur l'influence de l'une sur l'autre. Au regard des éléments énoncés ci-dessus, il paraît difficile que la refonte de la législation européenne ait lieu avant la fin du mandat de la présente Commission. Si les négociations dudit accord aboutissent avant cette refonte alors que cette dernière vise un renforcement des droits des citoyens européens, va-t-on réellement rouvrir les négociations avec les USA en appelant de nouveau à des standards de protection plus élevés ? Rien n'est moins sûr…

4. Renforcer les garanties en matière de protection des données dans le cadre de la coopération entre les services répressifs européens et américains.

La Commission européenne déclare que : « face à l'augmentation des volumes de données à caractère personnel collectées et traitées, les garanties juridiques et administratives applicables revêtent une importance d'autant plus grande. L'un des objectifs du groupe de travail *ad hoc* Union européenne-USA consiste à définir les garanties à appliquer pour réduire au minimum l'incidence du traitement des données à caractère personnel sur les droits fondamentaux des citoyens de l'Union européenne. »

Viser l'objectif de « limiter au maximum » l'incidence sur les droits fondamentaux n'est aucunement recevable.

5. Soutenir la réforme en cours aux États-Unis.

Suite aux révélations d'E. Snowden, le président américain Barack Obama a annoncé un réexamen des activités des autorités américaines chargées de la sécurité nationale et du cadre juridique en vigueur. La plus

van nationale veiligheid heeft reeds tot dergelijke grootschalige Amerikaanse observatieprogramma's geleid, zoals PRISM of het bespioneren van de Europese overheden door de NSA...

Het is dus erg waarschijnlijk dat de toekomstige waarborgen, zelfs wanneer ze worden bekrachtigd in de nieuwe overeenkomst over het kader voor de samenwerking op het vlak van rechtshandhaving, te licht zullen worden bevonden voor de uitdagingen die de Amerikaanse houding ten aanzien van de Europese wetgeving inzake gegevensbescherming oproept.

Overigens, aangezien die onderhandelingen tegelijkertijd werden opgestart met de intra-Europese onderhandelingen over gegevensbescherming, kunnen we ons afvragen hoe ze elkaar zullen beïnvloeden. In het licht van de bovenvermelde elementen, lijkt het weinig waarschijnlijk dat de herziening van de Europese wetgeving plaatsvindt vóór het einde van het mandaat van de huidige commissie. Indien de onderhandelingen over de voornoemde overeenkomst worden afgerond vóór die herziening, terwijl die laatste bedoeld is om de rechten van de Europese burgers te versterken, gaat men dan werkelijk de onderhandelingen met de VS heropstarten en opnieuw om hogere beschermingsstandaarden vragen ? Dat is zeer onwaarschijnlijk…

4. Versterking van de waarborgen inzake gegevensbescherming bij de samenwerking tussen de EU en de VS op het gebied van rechtshandhaving.

De Europese Commissie verklaart dat « de toename van de omvang van de verwerking van persoonsgegevens het belang [onderstreept] van de toepasselijke wettelijke en administratieve waarborgen. Een van de doelstellingen van de *ad-hoc*werkgroep van de EU en de VS bestond in de vaststelling welke waarborgen toepasselijk moeten zijn om de gevolgen van de verwerking voor de grondrechten van de EU-burgers zo klein mogelijk te houden. »

De doelstelling om de gevolgen voor de grondrechten « zoveel mogelijk te beperken » is geenszins aanvaardbaar.

5. Het lopende hervormingsproces in de Verenigde Staten steunen.

Na de onthullingen van E. Snowden, kondigde de Amerikaanse president Barack Obama een evaluatie aan van de activiteiten van de nationale veiligheidsinstanties van de VS, waarbij ook het toepasselijke rechtskader

grande modification consisterait ainsi dans l'application de ce dernier aux citoyens de l'Union européenne ne résidant pas aux États-Unis, ce qui leur offrirait les mêmes garanties que celles dont bénéficient les ressortissants et résidents américains.

Ceci représente toutefois certainement un vœu pieux, notamment au regard des récentes interventions du secrétaire d'État à la Justice Eric Holder et du directeur de la Sécurité nationale, James Clapper, qui ont précisé que Facebook, Google, LinkedIn, Microsoft, Yahoo ! et autres grands groupes, seraient autorisés à dévoiler « plus d'informations que jamais » sur leurs clients, notamment le nombre de comptes clients surveillés à la demande des agences de renseignement.

Benoit HELLINGS.

aan bod zal komen. Zo zou de grootste wijziging erin bestaan dat de waarborgen die burgers en inwoners van de VS nu genieten, ook gaan gelden voor niet in de VS woonachtige burgers van de EU.

Dat is vast en zeker een eerbiedige wens, in het bijzonder nadat de staatssecretaris van Justitie, Eric Holder, en de directeur van de Nationale Veiligheid, James Clapper, onlangs verklaarden dat Facebook, Google, LinkedIn, Microsoft, Yahoo ! en andere grote groepen « meer informatie dan ooit » zouden mogen bekendmaken over hun klanten, in het bijzonder het aantal klantenaccounts dat op vraag van inlichtingendiensten onder toezicht staat.

PROPOSITION DE RÉSOLUTION

Le Sénat

Considérant :

A. que le développement de l'économie numérique a entraîné une croissance exponentielle de la quantité, de la qualité, de la diversité et de la nature des activités de traitement de données ;

B. que l'utilisation de ces données et les méthodes modernes de traitement des données soulèvent des questions fondamentales, exacerbées dans le cadre des révélations relatives au programme américain de surveillance à grande échelle PRISM, mais également dans le cadre de l'affaire SWIFT ou des échanges de données passagers (PNR), dont le point commun est le potentiel dévastateur de ces programmes pour les droits fondamentaux des Européens en matière de protection de la vie privée, et qui mettent à mal les relations entre les États-Unis et l'Union européenne ;

C. qu'il existe déjà trois instruments qui structurent les relations entre les USA et l'Union européenne en matière de transfert de données : l'Accord PNR-*Passenger Name Record* (un accord d'entraide judiciaire sur l'utilisation et le transfert des données des dossiers des passagers (1)) à propos duquel la commission de l'Intérieur du Sénat a remis un avis critique, sur la base d'une proposition de résolution déposée par Ecolo et Groen (2) ; le TFTP-*Terrorist Finance Tracking Programme* (un accord sur le traitement et le transfert des données de messagerie financière aux fins du programme de surveillance du financement du terrorisme) et L'Accord entre Europol et les USA ;

D. qu'un quatrième accord-cadre sur la protection des données dans le domaine de la coopération policière et judiciaire visant à assurer un niveau élevé de protection des données est actuellement négocié entre l'Union européenne et les USA, avec l'objectif d'aboutir avant l'été 2014 ; que les négociations actuelles visent essentiellement la limitation des finalités, les conditions et la

(1) Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la sécurité intérieur.

(2) Proposition de résolution relative à la proposition de décision du Conseil européen relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation et le transfert des données des dossiers passagers (données PNR) au ministère américain de la Sécurité intérieure, Doc. Sénat n° 5-1534/1-2011/2012.

VOORSTEL VAN RESOLUTIE

De Senaat,

Overwegende :

A. dat de ontwikkeling van de digitale economie geleid heeft tot een exponentiële groei van de kwantiteit, de kwaliteit, de diversiteit en de aard van de gegevensverwerkingsactiviteiten ;

B. dat het gebruik van deze gegevens en moderne gegevensverwerkingsmethodes fundamentele vragen oproepen, die prangend zijn geworden sinds de onthullingen betreffende het grootschalige Amerikaanse bewakingsprogramma PRISM, maar ook sinds de zaak-SWIFT en de uitwisseling van passagiersgegevens (PNR), die gemeen hebben dat zij vernietigende gevolgen kunnen hebben voor de grondrechten van Europeanen inzake de bescherming van hun persoonlijke levenssfeer, en die de betrekkingen tussen de Verenigde Staten en de Europese Unie op de proef stellen ;

C. dat er reeds drie instrumenten voorhanden zijn die de betrekkingen tussen de Verenigde Staten en de Europese Unie op het vlak van gegevensoverdracht regelen : het PNR of *Passenger Name Record* (een overeenkomst betreffende gerechtelijke samenwerking op het vlak van het gebruik en de overdracht van passagiersgegevens (1) waarover de commmissie voor de Binnenlandse Zaken van de Senaat een kritisch advies heeft uitgebracht op grond van een voorstel van resolutie van Ecolo en Groen (2) ; het TFTP-*Terrorist Finance Tracking Programme* (een overeenkomst over de behandeling en de overdracht van financiële gegevens in het kader van de controle op de financiering van terrorisme) en de overeenkomst tussen Europol en de VS ;

D. dat er tussen de Europese Unie en de Verenigde Staten momenteel onderhandelingen aan de gang zijn over een vierde raamovereenkomst betreffende gegevensbescherming in politie- en gerechtelijke samenwerking teneinde een hoge graad van gegevensbescherming in te stellen, die voor de zomer van 2014 gesloten zou moeten zijn ; dat er onderhandelingen aan de gang zijn

(1) Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR-gegevens) aan het Amerikaanse ministerie van Binnenlandse Veiligheid.

(2) Voorstel van resolutie betreffende het voorstel voor een besluit van de Europese Raad tot sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR-gegevens) aan het Amerikaanse ministerie van Binnenlandse Veiligheid (stuk Senaat, nr. 5-1534/1-2011/2012).

durée de conservation des données ; mais qu'une définition restrictive des dérogations fondées sur des motifs de sécurité nationale ont déjà conduit aux dérives des programmes américains de surveillance comme PRISM ou l'espionnage des autorités publiques européennes par la NSA ;

E. qu'avant de transmettre ses communications COM(2013) 846 et COM(2013) 847, et face aux inquiétudes suscitées dans l'Union européenne par la collecte et le traitement à grande échelle d'informations à caractère personnel dans le cadre de programmes américains de surveillance, la Commission européenne a activé les mécanismes de révision conjointe permettant d'examiner la mise en œuvre des Accords PNR et TFTP ;

F. que pour l'Accord PNR, le rapport de la Commission européenne (1) constate qu'une plus grande transparence est nécessaire dans le droit d'accès des citoyens à leurs données sans exception, que la durée de conservation avant dépersonnalisation des données dépasse les six mois prévus dans l'Accord, qu'il y a recours trop systématique à la méthode « *push* » alors qu'elle devrait être occasionnelle, et par conséquent, la Commission recommande de renouveler un examen conjoint rapidement ;

G. que pour l'Accord TFTP, une consultation officielle a généré un engagement écrit des États-Unis assurant qu'aucune collecte directe de données n'avait lieu en violation de l'Accord et que la nécessité d'un tel écrit pose question, vu qu'un tel engagement est déjà contenu dans l'Accord, et que de plus, ceci n'empêche pas la Commission d'avancer le prochain examen conjoint ;

H. qu'en ce qui concerne l'Accord Europol-USA, l'autorité de contrôle commune (ACC) a procédé, en novembre 2011, à un deuxième contrôle de la mise en œuvre des tâches d'Europol au titre de l'accord TFTP (2). Et que si la situation s'est améliorée par rapport à l'an passé, l'ACC affirme qu'il reste encore beaucoup à faire dans de nombreux domaines (les demandes doivent mieux justifier la nécessité du champ géographique choisi, les catégories de données à caractère personnel demandées et les données effectivement contenues dans chaque type de message demandé) ;

(1) *Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security*, COM(2013) 844 final.

(2) L'ACC d'Europol contrôle pour la deuxième année la mise en œuvre de l'accord TFTP1, Déclaration publique, Bruxelles, 14 mars 2012.

betreffende de beperking van de finaliteiten, de voorwaarden en de bewaringsduur van gegevens ; maar dat een restrictieve definitie van de uitzonderingen om redenen van nationale veiligheid al hebben geleid tot misbruiken door Amerikaanse programma's als PRISM of het bespioneren van Europese overheden door de NSA ;

E. dat de Europese Commissie, alvorens mededelingen COM(2013) 846 en COM(2013) 847 bekend te maken, en bezorgd om de grootschalige verzameling en behandeling van persoonsgegevens door Amerikaanse bewakingsprogramma's, de gezamenlijke herzieningsmechanismen heeft geactiveerd om de tenuitvoerlegging van PNR- en TFPT-Overeenkomsten te onderzoeken ;

F. dat voor de PNR-overeenkomst, het verslag van de Europese Commissie (1) vaststelt dat er meer transparantie vereist is in het recht van de burger op toegang tot hun gegevens zonder uitzondering, dat de bewaringstermijn vóór de ontpersoonlijking van gegevens langer is dan de zes maanden die de Overeenkomst voorschrijft, dat er te systematisch gebruik wordt gemaakt van de « *push* »-methode, terwijl dit slechts occasioneel zou mogen gebeuren, en dat de Commissie bijgevolg aanbeveelt een gezamenlijk onderzoek snel opnieuw uit te voeren ;

G. dat voor de TFPT-Overeenkomst, een officiële raadpleging is uitgemond in een schriftelijke verbintenis van de Verenigde Staten dat geen enkele rechtstreekse gegevensverzameling had plaatsgevonden die in strijd was met de Overeenkomst en dat de noodzaak van een dergelijk geschrift vragen oproept, aangezien een dergelijke verbintenis reeds in de Overeenkomst was vervat, en dat het bovendien niet belet dat de Commissie overgaat tot het volgende gezamenlijk onderzoek ;

H. dat wat de Overeenkomst Europol-USA betreft, de Gemeenschappelijke Controle Autoriteit (GCA) in november 2001 een tweede controle heeft uitgevoerd van de tenuitvoerlegging van de opdrachten van Europol in het raam van de TFTP-Overeenkomst (2). En dat hoewel de situatie is verbeterd ten opzichte van vorig jaar, de GCA oordeelt dat er nog veel te doen is op vele vlakken (de aanvragen moeten een omstandiger verantwoording geven van de noodzaak van het gekozen geografisch veld, de categorieën van de opgevraagde persoonsgegevens en de gegevens die daadwerkelijk vervat zijn in elk soort opgevraagd bericht) ;

(1) *Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security,* COM(2013) 844 final.

(2) Europol-GCO inspecteert voor het tweede jaar de uitvoering van de TFTP-Overeenkomst, Openbare verklaring, Brussel, 14 maart 2012.

I. qu'il existe actuellement deux instruments multilatéraux importants pour encadrer les transferts de données personnelles dans un contexte commercial : la directive 95/46 qui fixe les règle applicables au transfert de données à caractères personnel des États membres vers des pays tiers dans la mesure où des « décisions constatent du caractère adéquat du niveau de protection » dans le pays tiers ; et la décision (1) relative à la « sphère de sécurité » qui autorise le libre transfert d'informations à caractère personnel des États membres de l'Union européenne vers des entreprises établies aux USA qui se sont engagées à respecter les principes de la sphère de sécurité ;

J. que « le rapport de la Commission sur le fonctionnement de la sphère de sécurité met en évidence un certain nombre d'insuffisances », et que parmi les lacunes qui affectent la transparence et l'exécution de cet accord, la Commission européenne relève les points tels que fausses déclarations d'adhésion, absence d'intégration dans le fonctionnement des entreprises, absence de contrôle effectif, exclusion du champ de la sphère de sécurité des entreprises de télécommunications pourtant porteuses d'un nombre important de données à caractère personnel, absence d'obligation pour les tiers responsables de traitement que sont les sous-traitants ;

K. que la Commission européenne déclare elle-même qu'il « convient également de disposer de garanties pour protéger les entreprises. En vertu de certaines lois américaines, comme le *Patriot Act*, les autorités américaines peuvent directement s'adresser à des entreprises pour solliciter l'accès à des données stockées dans l'Union européenne. En conséquence, des entreprises européennes, et des entreprises américaines établies dans l'Union européenne, peuvent se voir contraintes de transférer des données vers les États-Unis en violation du droit de l'Union européenne et des législations des États membres et se trouvent ainsi confrontées à un conflit d'obligations juridiques » ;

L. que par ses communications et les évaluations déjà disponibles de certains instruments encadrant les échanges transatlantiques de données personnelles, la Commission européenne atteste que les cadres législatifs en chantier mettent à mal et, dans certains cas, ne permettent pas de respecter les droits acquis des citoyens européens en matière de protection des données à caractère personnel,

(1) Décision 2000/520/CE.

I. dat er momenteel twee belangrijke multilaterale instrumenten bestaan om de overdracht van persoonsgegevens te regelen in een commerciële context : richtlijn 95/46 die de regels vaststelt voor de overdracht van persoonsgegevens van de lidstaten naar derde landen, waarbij het « passend karakter van het door een derde land geboden beschermingsniveau » in aanmerking wordt genomen ; en de beschikking (1) betreffende de bescherming geboden door de « veiligehavenbeginselen » voor de vrije overdracht van persoonsgegevens van de lidstaten van de Europese Unie naar bedrijven in de Verenigde Staten die zich ertoe verbonden hebben deze beginselen na te leven ;

J. dat het verslag van de Commissie over de werking van de veilige haven een aantal tekortkomingen aanhaalt die de transparantie en de uitvoering belemmeren, waaronder valse toetredingsverklaringen, geen toepassing van de beginselen in de praktijk door bedrijven, geen daadwerkelijke controle, het feit dat telecombedrijven, die nochtans vele persoonsgegevens overbrengen, buiten het toepassingsgebied van de veiligehavenregeling vallen, het gebrek aan verplichtingen voor derden die verantwoordelijk zijn voor de verwerking, met name de onderaannemers ;

K. dat de Europese Commissie zelf het volgende verklaart : « Ook voor de bescherming van ondernemingen zijn waarborgen noodzakelijk. Op grond van bepaalde wetten in de VS, zoals de *Patriot Act*, kunnen de Amerikaanse autoriteiten ondernemingen rechtstreeks verzoeken om toegang tot in de EU opgeslagen gegevens. Van Europese ondernemingen en in de EU aanwezige Amerikaanse ondernemingen kan daarom worden verlangd dat zij in strijd met de wetgeving van de EU en de lidstaten gegevens aan de VS doorgeven en zij zijn dan ook permanent gevangen tussen met elkaar strijdige wettelijke verplichtingen. » ;

L. dat in haar mededelingen en de reeds beschikbare evaluaties van een aantal instrumenten die de uitwisseling van transatlantische persoonsgegevens omkaderen, de Europese Commissie bevestigt dat de wetgevende kaders die in de maak zijn de verworven rechten van de Europese burgers inzake de bescherming van persoonsgegevens aantasten en soms schenden,

(1) Besluit 2000/520/EG.

Demande au gouvernement de faire connaître à la Commission européenne ses demandes de voir :

1. la Commission s'engager à réformer, dans les plus brefs délais et avec comme seuls objectifs la sauvegarde de la vie privée des citoyens européens, les règles de l'Union européenne en matière de protection des données, afin que la renégociation des accords en cours avec les États-Unis puissent s'appuyer sur des standards particulièrement élevés de protection des données à caractère personnel ;

2. la Commission exiger, avant la signature de l'Accord entre services répressifs, que les États-Unis soient membres de la Convention du Conseil de l'Europe pour la protection à l'égard du traitement automatisé des données à caractère personnel (Convention 108) qui est ouverte aux pays qui ne sont pas membres du Conseil de l'Europe ;

3. la Commission garantir les droits acquis des citoyens de l'Union européenne et affirmer que son objectif est de définir les garanties à appliquer pour réduire absolument l'incidence du traitement des données à caractère personnel sur les droits fondamentaux des citoyens de l'Union européenne ;

4. suspendre l'accord dit de « sphère de sécurité » entre l'Union européenne et les États-Unis tant que ces derniers n'appliquent pas une législation comparable à celle de l'Union européenne en matière de protection de données et qu'il soit ainsi mis fin à ces conflits d'obligations juridiques rencontrés par les entreprises américaines, comme l'ont déjà demandé les parlementaires européens. En effet, le Parlement européen a appelé, le 15 janvier dernier, lors d'un débat en plénière, la Commission européenne à suspendre immédiatement l'Accord mis en cause dans la foulée sur le scandale PRISM puis sur les écoutes de l'Agence américaine de sécurité nationale (NSA). Par ailleurs, Jan Philipp Albrech, député européen et membre de la Commission LIBE, rappelle, lors de cette même séance plénière, que « *If we do not stop the circumvention of European rules by US companies by passing our single data protection regulation and putting pressure on the United States — and also by cancelling the Safe Harbour decision — we will not only lose the sovereignty of the European Union but we will also lose the voters, who will stay at home, as they do not expect us to protect their interests and rights* ».

Vraagt de regering aan de Europese Commissie haar volgende verzoeken mede te delen :

1. dat de Commissie zich ertoe verbindt om zo snel mogelijk en met als enig doel het vrijwaren van de private levenssfeer van de Europese burgers, de regels van de Europese Unie inzake gegevensbescherming te hervormen zodat de huidige heronderhandeling van de overeenkomsten met de Verenigde Staten kunnen stoelen op bijzonder hoge standaarden inzake bescherming van persoonsgegevens ;

2. dat de Commissie vóór de ondertekening van de Overeenkomst tussen repressieve diensten eist dat de Verenigde Staten zich aansluiten bij het Verdrag van de Raad van Europa tot bescherming van de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108), dat openstaat voor landen die geen lid zijn van de Raad van Europa ;

3. dat de Commissie de verworven rechten van de burgers van de Europese Unie waarborgt en bevestigt dat zij ernaar streeft de waarborgen te bepalen die nodig zijn om volledig te voorkomen dat de verwerking van persoonsgegevens inbreuk doet op de fundamentele rechten van de burgers van de Europese Unie ;

4. dat de overeenkomst betreffende de zogenaamde « veilige haven » tussen de Europese Unie en de Verenigde Staten wordt opgeschort zolang de VS geen wetgeving inzake databescherming toepast die vergelijkbaar is met die van de Europese Unie, en dat er zo een einde wordt gemaakt aan de conflicten betreffende juridische verplichtingen die Amerikaanse ondernemingen ondervinden, zoals de Europese parlementsleden reeds hebben gevraagd. Het Europees Parlement heeft op 15 januari jongstleden, tijdens een bespreking in de plenaire vergadering, de Europese Commissie immers opgeroepen om onmiddellijk de Overeenkomst op te schorten ten gevolge van het PRISM-schandaal en de onthullingen over de afluisterpraktijken van het Amerikaans veiligheidsagentschap NSA. Tijdens diezelfde plenaire vergadering heeft Jan Philipp Albrech, europarlementslid en lid van de LIBE-Commissie, bovendien verklaard dat « *If we do not stop the circumvention of European rules by US companies by passing our single data protection regulation and putting pressure on the United States — and also by cancelling the Safe Harbour decision — we will not only lose the sovereignty of the European Union but we will also lose the voters, who will stay at home, as they do not expect us to protect their interests and rights* ».

Ceci à l'image des commissaires allemands à la protection des données qui ont décidé de ne plus délivrer d'autorisations de transfert de données vers des pays tiers (par exemple, pour l'utilisation de certains services en nuage ou cloud) et qui examineront également s'il convient de suspendre les transferts de données dans le cadre de la sphère de sécurité (1), activer l'article 3 de la décision relative à la sphère de sécurité qui autorise les autorités européennes à suspendre, sous certaines conditions, les flux de données vers des entreprises adhérant aux principes de la sphère de sécurité (2) ;

5. suspendre des négociations en cours en vue de la conclusion d'un Partenariat transatlantique de commerce et d'investissements tant qu'il n'apporte pas les garanties suffisantes, surtout au regard de la présente analyse, quant au respect intégral des normes de l'Union dans le domaine de la protection des données, y compris celles sur les transferts internationaux. En effet, la Commission européenne fait fi de cette actualité en la balayant d'un revers de manche et déclare ainsi que les normes de protection des données à caractère personnel doivent être examinées dans un contexte propre, sans que cela n'affecte d'autres dimensions des relations entre l'Union et les États-Unis, notamment les négociations en cours pour un partenariat transatlantique. Or, si l'Union européenne négocie avec un partenaire qui l'espionne, la négociation n'est ni juste ni équilibrée. Or, c'est que que les États-Unis sont occupés à faire.

11 mars 2014.

Benoit HELLINGS.

(1) *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, communiqué de presse du 24 juillet 2013.

(2) En vertu de l'article 3 de la décision relative à la sphère de sécurité, ce type de suspensions peuvent être appliquées dans les cas où il est fort probable que les principes sont violés ; où il y a tout lieu de croire que l'instance d'application concernée ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question ; où la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves ; et où les autorités compétentes des États membres se sont raisonnablement efforcées, compte tenu des circonstances, d'avertir l'organisation et de lui donner la possibilité de répondre.

Zo hebben de Duitse commissieleden voor databescherming besloten geen vergunningen voor gegevensoverdracht naar derde landen meer uit te reiken (bijvoorbeeld voor het gebruik van sommige cloud-diensten) en zullen zij nagaan of ook de gegevensoverdracht in het kader van de veilige haven geschorst moet worden (1) met toepassing van artikel 3 van de beschikking betreffende de veiligehavenbeginselen dat de Europese overheid in staat stelt om onder bepaalde voorwaarden de gegevensstromen naar bedrijven die de veiligehavenbeginselen onderschrijven, te schorsen (2) ;

5. dat de huidige onderhandelingen voor het sluiten van een transatlantisch Partnerschap voor handel en investeringen worden opgeschort zolang het, zeker gelet op de onderhavige analyse, onvoldoende voorwaarden biedt voor een volledige naleving van de Europese normen inzake databescherming, met inbegrip van de normen betreffende internationale overdrachten. De Europese Commissie houdt immers geen rekening met deze actualiteit door ze te negeren en verklaart aldus dat de beschermingsnormen van persoonsgegevens beschouwd moeten worden in hun eigen context, zonder dat zij invloed hebben op andere aspecten van de betrekkingen tussen de Unie en de Verenigde Staten, waaronder de lopende onderhandelingen voor een transatlantisch partnerschap. Maar als de Europese Unie onderhandelt met een partner die haar bespioneert, is de onderhandeling noch eerlijk, noch evenwichtig. Dat is echter wat de Verenigde Staten aan het doen zijn.

11 maart 2014.

(1) *Bundesbeauftragten für den Datenschutz und die Informationsfreihei*t, persbericht van 24 juli 2013.

(2) Krachtens artikel 3 van de beschikking betreffende de veiligehavenbeginselen, kan dit soort opschorting toegepast worden in de gevallen dat « het zeer waarschijnlijk is dat de beginselen worden geschonden ; er redelijkerwijs kan worden aangenomen dat het desbetreffende handhavingsmechanisme niet tijdig passende maatregelen neemt of zal nemen om het betrokken probleem op te lossen ; zich een risico voordoet dat de betrokkenen ernstige schade wordt toegebracht wanneer verder gegevens worden doorgegeven ; en de bevoegde autoriteiten in de lidstaat zich naar omstandigheden redelijke inspanningen hebben getroost om de organisatie van het probleem in kennis te stellen en de gelegenheid te geven te reageren ».

Centrale drukkerij – Imprimerie centrale