COMMISSION
EUROPÉENNE

Bruxelles, le 27.11.2013
COM(2013) 847 final

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

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

1. INTRODUCTION

La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après la «directive sur la protection des données») fixe les règles applicables au transfert de données à caractère personnel des États membres de l'Union européenne vers des pays tiers[1], dans la mesure où ces transferts relèvent du champ d'application dudit instrument[2].

En vertu de cette directive, la Commission peut constater qu'un pays tiers assure un niveau de protection adéquat en raison de sa législation interne ou des engagements internationaux auxquels il a souscrit pour protéger les droits des personnes, auquel cas les limitations prévues ne s'appliquent pas aux transferts de données vers ce pays. Ces décisions sont généralement dénommées «**décisions constatant le caractère adéquat du niveau de protection**».

Le 26 juillet 2000, la Commission a adopté la décision 2000/520/CE[3] (ci-après la «**décision relative à la sphère de sécurité**») reconnaissant les principes de la «sphère de sécurité» et les questions souvent posées y afférentes (dénommés respectivement les «principes» et les «FAQ» - *frequently asked questions*), publiés par le ministère du commerce des États-Unis d'Amérique, comme assurant un niveau de protection adéquat aux fins des transferts de données à caractère personnel depuis l'UE. La décision relative à la sphère de sécurité a été arrêtée à la suite d'un avis du groupe de travail «article 29» et d'un avis du comité de l'article 31 rendu à la majorité qualifiée des États membres. Conformément à la décision 1999/468/CE du Conseil, la décision relative à la sphère de sécurité avait été préalablement soumise à l'examen approfondi du Parlement européen.

En conséquence, l'actuelle décision relative à la sphère de sécurité autorise le libre transfert[4] d'informations à caractère personnel des États membres de l'UE[5] vers des entreprises établies aux États-Unis qui se sont engagées à respecter les principes de la sphère de sécurité dans les cas où le transfert ne satisferait pas autrement aux normes de l'UE en matière d'adéquation du niveau de protection des données, compte tenu des différences substantielles existant entre les régimes de protection de la vie privée de part et d'autre de l'Atlantique.

Le fonctionnement de l'actuel accord sur la sphère de sécurité repose sur les engagements pris par les entreprises qui décident d'y souscrire et l'autocertification de celles-ci. L'adhésion revêt

---

1 Les articles 25 et 26 de la directive sur la protection des données établissent le cadre juridique des transferts de données à caractère personnel de l'UE vers des pays tiers ne faisant pas partie de l'EEE.

2 Des règles supplémentaires ont été définies à l'article 13 de la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, dans la mesure où ces transferts concernent des données à caractère personnel transmises à un autre État membre ou mises à sa disposition, lequel entend ensuite les transmettre à un État tiers ou une instance internationale 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.

3 Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de 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 d'Amérique, JO L 215 du 25.8.2000, p. 7.

4 Ce qui précède n'exclut pas l'application au traitement de données d'autres exigences qui peuvent exister en vertu de la législation nationale transposant la directive européenne sur la protection des données.

5 Les transferts de données depuis les trois États parties à l'EEE sont également concernés, à la suite de l'extension de la directive 95/46/CE à l'accord EEE par la décision n° 83/1999 du 25 juin 1999, JO L 296 du 23.11.2000, p. 41.

un caractère volontaire, mais les règles sont contraignantes pour les entreprises qui y souscrivent. Les principes fondamentaux de cet accord sont les suivants:

a) transparence des politiques de protection de la vie privée adoptées par les entreprises qui adhèrent aux principes,

b) intégration des principes de la sphère de sécurité dans les politiques de protection de la vie privée adoptées par les entreprises, et

c) mise en œuvre, y compris par les autorités publiques.

Or ces fondements de la sphère de sécurité doivent être réexaminés au vu du **contexte actuel**, caractérisé par:

a) la croissance exponentielle des flux de données, autrefois accessoires, mais désormais au cœur de la rapide croissance de l'économie numérique et des grandes évolutions en matière de collecte, de traitement et d'utilisation des données,

b) l'importance cruciale des flux de données, notamment pour l'économie transatlantique[6],

c) la rapide croissance du nombre d'entreprises établies aux États-Unis qui souscrivent au régime de la sphère de sécurité, nombre qui a été multiplié par huit depuis 2004 (passant de 400 en 2004 à 3 246 en 2013),

d) les informations récemment diffusées sur les programmes de surveillance américains, qui soulèvent de nouvelles questions quant au niveau de protection que l'accord sur la sphère de sécurité est censé garantir.

Dans ce contexte, la présente communication fait le point sur le fonctionnement du régime de la sphère de sécurité. Elle est **fondée sur des éléments** recueillis par la Commission, les travaux du groupe de contact UE/États-Unis sur la protection de la vie privée menés en 2009, une étude réalisée en 2008 par un contractant indépendant[7] et les informations reçues par le groupe de travail ad hoc UE/États-Unis (ci-après dénommé le «groupe de travail»), créé à la suite des révélations sur les programmes de surveillance américains *(voir un document parallèle)*. La présente communication fait suite à **deux rapports d'analyse d'impact de la Commission**, présentés respectivement en 2002[8] et en 2004[9], durant la phase de démarrage de l'accord sur la sphère de sécurité.

2. STRUCTURE ET FONCTIONNEMENT DE LA SPHERE DE SECURITE

2.1. Structure de la sphère de sécurité

Une entreprise américaine souhaitant adhérer aux principes de la sphère de sécurité est tenue de: a) stipuler, dans sa politique de protection de la vie privée, qu'elle rend publique, qu'elle

[6] D'après certaines études, si les services et les flux de données transatlantiques devaient être perturbés en raison de la suppression des règles d'entreprise contraignantes, des clauses contractuelles types et de la sphère de sécurité, l'impact négatif sur le PIB de l'UE pourrait être compris entre -0,8 % et -1,3 %, et les exportations de services de l'UE vers les États-Unis enregistreraient un recul de 6,7 %, imputable à une perte de compétitivité. Voir: «*The Economic Importance of Getting Data Protection Right*», étude réalisée par le European Centre for International Political Economy (ECIPE) pour le compte de l'U.S. Chamber of Commerce, mars 2013.

[7] Rapport d'analyse d'impact établi en 2008, pour le compte de la Commission européenne, par le *Centre de Recherche Informatique et Droit* (CRID) de l'université de Namur.

[8] Document de travail des services de la Commission intitulé «L'application de la décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de 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 d'Amérique», SEC(2002) 196 du 13.12.2002.

[9] Document de travail des services de la Commission intitulé «La mise en œuvre de la décision 2000/520/CE de la Commission relative à la pertinence de 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 d'Amérique», SEC(2004) 1323 du 20.10.2004.

adhère auxdits principes et s'y conforme effectivement, et de b) s'autocertifier, c'est-à-dire de déclarer au ministère du commerce qu'elle est en conformité avec lesdits principes. L'autocertification doit être annuellement renouvelée. Les principes de la «sphère de sécurité» relatifs à la protection de la vie privée, joints en annexe I de la décision relative à la sphère de sécurité, incluent des exigences en ce qui concerne, d'une part, la protection matérielle des données à caractère personnel (principes d'intégrité des données, de sécurité, de choix et de transfert ultérieur) et, d'autre part, les droits procéduraux des personnes concernées par les données (principes de notification, d'accès et d'application).

Pour ce qui est de la mise en œuvre du régime de la sphère de sécurité aux États-Unis, deux institutions américaines jouent un rôle prépondérant: le ministère du commerce des États-Unis d'Amérique (*US Department of Commerce*) et la Commission fédérale du commerce (*US Federal Trade Commission* ou FTC).

Le **ministère du commerce** examine toutes les autocertifications effectuées dans le cadre de la sphère de sécurité ainsi que tous les renouvellements annuels de celles-ci que les entreprises lui soumettent, afin de s'assurer qu'ils contiennent bien tous les éléments requis par l'adhésion au régime[10]. Il met à jour la liste des entreprises qui lui ont adressé des lettres d'autocertification et publie cette liste et ces lettres sur son site web. En outre, il contrôle le fonctionnement de la sphère de sécurité et radie de la liste les entreprises qui ne se conforment pas ou plus à ses principes.

La **Commission fédérale du commerce**, dans le cadre de ses compétences en matière de protection des consommateurs, cible les pratiques déloyales ou frauduleuses, conformément à l'article 5 de la loi sur la Commission du libre-échange. Dans le cadre de ses actions de contrôle de l'application, la Commission fédérale du commerce enquête sur les fausses déclarations d'adhésion à la sphère de sécurité et sur le non-respect de ses principes par des entreprises qui en sont membres. Dans les cas spécifiques où il s'agit d'opposer les principes de la sphère de sécurité à des transporteurs aériens, l'autorité compétente est le ministère américain des transports[11].

L'actuelle décision relative à la sphère de sécurité fait partie du droit de l'UE qui doit être appliqué par les autorités des États membres. En vertu de cette décision, les **autorités chargées de la protection des données** (DPA) des États membres de l'UE ont le droit, dans certains cas, de suspendre les transferts de données vers des entreprises certifiées dans le cadre de la sphère de sécurité[12]. La Commission n'a pas connaissance de cas de suspension par une autorité nationale chargée de la protection des données depuis la mise en place de la sphère de sécurité en 2000. Indépendamment des pouvoirs dont elles jouissent en vertu de la décision relative à la sphère de sécurité, les autorités des États membres chargées de la protection des données ont compétence pour intervenir, y compris dans le cas de transferts internationaux, afin de veiller au respect des principes généraux de la protection des données qui sont énoncés dans la directive de 1995 sur la protection des données.

Ainsi que le rappelle l'actuelle décision relative à la sphère de sécurité, il est de **la compétence de la Commission** – agissant conformément à la procédure d'examen définie

---

10 Si la certification d'une entreprise ou son renouvellement ne satisfait pas ou plus aux exigences de la sphère de sécurité, le ministère du commerce le notifie à l'entreprise concernée et l'invite à prendre des mesures de mise en conformité (par exemple, préciser ou modifier ses dispositions de protection de la vie privée), de sorte que la procédure de certification puisse aboutir.

11 En vertu du titre 49 du US Code (code de réglementations fédérales des États-Unis), article 41712.

12 Concrètement, la suspension des transferts peut être exigée dans deux cas de figure, à savoir dans les cas:
a) où l'organe administratif américain constate que l'entreprise viole les principes de la sphère de sécurité; ou
b) 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'entreprise et de lui donner la possibilité de répondre.

dans le règlement n° 182/2011 – d'adapter la décision, de la suspendre ou d'en limiter la portée à tout moment, à la lumière de l'expérience acquise durant sa mise en œuvre. Cela est notamment prévu en cas de défaillance systémique de la part des autorités américaines, par exemple, si une autorité chargée de veiller au respect des principes de la sphère de sécurité aux États-Unis ne remplit pas effectivement son rôle, ou si les exigences du droit américain l'emportent sur les principes de la sphère de sécurité. Comme toute autre décision de la Commission, elle peut également être modifiée pour d'autres motifs, voire abrogée.

2.2. Le fonctionnement de la sphère de sécurité

Les **3 246**[13] **entreprises certifiées** sont à la fois des petites et des grandes entreprises[14]. Alors que les secteurs des services financiers et des télécommunications ne relèvent pas des pouvoirs d'exécution de la Commission fédérale du commerce et sont, dès lors, exclus de la sphère de sécurité, de nombreux secteurs de l'industrie et des services sont représentés parmi les entreprises certifiées, dont des entreprises très connues du secteur de l'internet, secteurs qui vont des services informatiques aux produits pharmaceutiques, en passant par les services touristiques et de voyages, les soins de santé et les services de cartes de crédit[15]. Il s'agit principalement d'entreprises américaines qui fournissent des services sur le marché intérieur de l'UE, mais aussi de filiales d'entreprises de l'UE telles que Nokia ou Bayer. 51 % d'entre elles sont des entreprises qui traitent des données concernant des salariés employés en Europe, lesquelles sont transférées vers les États-Unis à des fins de gestion des ressources humaines[16].

Certaines autorités des États membres de l'UE chargées de la protection des données se montrent **de plus en plus préoccupées** par les transferts de données effectués dans le cadre actuel de la sphère de sécurité. Certaines d'entre elles émettent des critiques à l'égard de la formulation très générale des principes et du fait que le cadre actuel repose largement sur l'autocertification et l'autorégulation. Des préoccupations du même ordre sont exprimées par des entreprises qui signalent des distorsions de concurrence liées à un contrôle insuffisant du respect des principes de la sphère de sécurité.

L'actuel accord relatif à la sphère de sécurité est fondé sur l'adhésion volontaire des entreprises aux principes, sur l'autocertification des entreprises adhérant aux principes et sur le contrôle par les autorités publiques du respect des engagements pris lors de l'autocertification. Dans ce contexte, tout défaut de transparence et toute lacune dans la mise en œuvre et son contrôle peuvent saper les fondements sur lesquels est construit le régime de la sphère de sécurité.

En effet, tout défaut et toute lacune de ce type du côté américain ont pour effet de reporter la responsabilité sur les autorités européennes chargées de la protection des données et sur les entreprises qui appliquent ce régime. Le 29 avril 2010, les autorités allemandes chargées de la protection des données ont rendu une décision demandant aux entreprises qui transfèrent des données de l'Europe vers les États-Unis, de vérifier attentivement que les entreprises américaines important des données respectent effectivement les principes de la sphère de sécurité, et formulant la recommandation suivante: «l'entreprise exportatrice des données doit

---

13 Le 26 septembre 2013, le nombre d'organisations adhérentes à la sphère de sécurité dont la certification était «**à jour**» sur la liste de la sphère de sécurité était de **3 246**, contre **935** pour celles dont la certification n'était «**plus à jour**».

14 Organisations de la sphère de sécurité comptant jusqu'à 250 salariés: **60 %** (1 925 sur 3 246). Organisations de la sphère de sécurité comptant au moins 251 salariés: **40 %** (1 295 sur 3 246).

15 À titre d'exemple, MasterCard traite avec des milliers de banques et constitue un bon exemple de cas dans lequel la sphère de sécurité ne peut être remplacée par d'autres instruments juridiques aux fins des transferts de données à caractère personnel tels que des règles d'entreprise contraignantes ou des dispositions contractuelles.

16 Organisations de la sphère de sécurité qui traitent des données relatives aux ressources humaines en vertu de leur certification dans le cadre la sphère de sécurité (et ont, en conséquence, accepté de se conformer aux principes et de coopérer avec les autorités de l'UE chargées de la protection des données): **51 %** (1 671 sur 3 246).

au moins déterminer si la certification de l'importateur des données dans le cadre de la sphère de sécurité est toujours valable»[17].

Le 24 juillet 2013, à la suite des révélations sur les programmes de surveillance américains, les autorités allemandes chargées de la protection des données ont franchi un pas de plus en exprimant leur préoccupation en ces termes: «il est fort probable que les principes énoncés dans les décisions de la Commission soient violés»[18]. Il est arrivé que des autorités chargées de la protection des données (par exemple, l'autorité de Brême) demandent à une entreprise transférant des données à caractère personnel à des fournisseurs américains, de les informer de la manière dont lesdits fournisseurs (pour autant que ce soit effectivement le cas) empêchent l'Agence nationale de sécurité d'accéder à ces données. L'autorité irlandaise chargée de la protection des données a signalé qu'elle avait récemment été saisie de deux plaintes relatives au programme de la sphère de sécurité, à la suite des articles publiés sur les programmes des agences de renseignement américaines, mais qu'elle avait refusé de les traiter au motif que ce transfert de données à caractère personnel vers un pays tiers satisfaisait aux exigences de la législation irlandaise en matière de protection des données. À la suite d'une plainte similaire, l'autorité luxembourgeoise chargée de la protection des données a conclu que les entreprises Microsoft et Skype respectaient la loi luxembourgeoise relative à la protection des données lorsqu'elles transféraient des données vers les États-Unis[19]. En revanche, la High Court irlandaise a, depuis lors, fait droit à une demande de contrôle juridictionnel dans le cadre duquel elle examinera l'inaction du commissaire irlandais à la protection des données à l'égard des programmes américains de surveillance. L'une de ces deux plaintes avait été déposée par un groupe d'étudiants dénommé «Europe versus Facebook» (EvF), qui a également déposé une plainte similaire contre Yahoo en Allemagne, laquelle est actuellement examinée par les autorités compétentes en matière de protection des données.

Ces réactions divergentes des autorités chargées de la protection des données aux révélations sur les programmes américains de surveillance démontrent le risque réel de fragmentation du cadre de la sphère de sécurité et soulèvent des questions quant à la mesure dans laquelle il peut être mis en œuvre.

---

17 Voir la décision du Düsseldorfer Kreis des 28/29 avril 2010. Voir: *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover*: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile Toutefois, M. Peter Hustinx, contrôleur européen de la protection des données (CEPD), a déclaré, lors de l'audience publique du 7 octobre 2013 consacrée à une enquête de la commission LIBE du Parlement européen, que «des améliorations conséquentes [avaient] été apportées et que la plupart des problèmes [avaient] désormais été réglés» en ce qui concerne la sphère de sécurité: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_FR.pdf

18 Voir la résolution d'une conférence allemande des commissaires à la protection des données dont il ressort que les services de renseignement représentent une menace considérable pour la transmission de données entre l'Allemagne et des pays non-européens: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 Voir le communiqué de presse, du 18 novembre 2013, de l'autorité luxembourgeoise chargée de la protection des données.

3. LA TRANSPARENCE DES POLITIQUES DE PROTECTION DE LA VIE PRIVEE ADOPTEES PAR LES ENTREPRISES ADHERANT A LA SPHERE DE SECURITE

Selon la FAQ 6 figurant en annexe de la décision relative à la sphère de sécurité (annexe II), les entreprises souhaitant certifier leur adhésion à la sphère de sécurité doivent communiquer leur politique de protection de la vie privée au ministère du commerce et la rendre publique. Cette politique doit comprendre un engagement à respecter les principes de protection de la vie privée. L'obligation faite aux entreprises autocertifiées de **rendre publiques leurs dispositions de protection de la vie privée** et de déclarer leur adhésion aux principes de protection de la vie privée sont des éléments indispensables au fonctionnement du cadre.

Le manque d'accessibilité à ces dispositions porte préjudice aux personnes dont les données à caractère personnel sont collectées et traitées et il peut constituer une **violation du principe de notification**. En pareil cas, il peut arriver que les personnes dont les données sont transférées à partir de l'UE ignorent leurs droits et n'aient pas connaissance des obligations incombant aux entreprises autocertifiées.

De plus, l'engagement pris par les entreprises de se conformer aux principes de protection de la vie privée **fonde la commission fédérale du commerce à exercer ses pouvoirs pour opposer ces principes** aux entreprises qui, en adoptant des pratiques déloyales ou frauduleuses, ne les observent pas. Le manque de transparence qui caractérise les entreprises aux États-Unis complique la surveillance exercée par la commission fédérale du commerce et nuit à l'efficacité du contrôle de l'application de ces principes.

Au fil des ans, un nombre important d'entreprises autocertifiées n'ont pas publié leur politique de protection de la vie privée et/ou n'ont pas fait de déclaration publique quant à leur adhésion aux principes de protection de la vie privée. Le rapport de 2004 sur la sphère de sécurité a souligné la nécessité que le ministère du commerce **adopte une approche plus active pour le contrôle du respect** de cette exigence.

Depuis 2004, ce ministère a mis au point **de nouveaux outils d'information** destinés à aider les entreprises à se conformer à leurs obligations en matière de transparence. Le site web du ministère consacré au cadre de la sphère de sécurité[20] fournit les informations utiles à cet égard et permet aussi aux entreprises de télécharger leurs dispositions en matière de protection de la vie privée. Le ministère a indiqué que des entreprises avaient fait usage de cette possibilité et publié leurs dispositions de protection de la vie privée sur son site web lors de leur demande d'adhésion à la sphère de sécurité[21]. En outre, il a publié entre 2009 et 2013 une série de lignes directrices à l'intention des entreprises souhaitant adhérer à la sphère de sécurité, comme le «*Guide to Self-Certification*» (guide de l'autocertification) et la brochure «*Helpful Hints on Self-Certifying Compliance*» (conseils utiles pour une autocertification conforme)[22].

Le degré de respect des obligations en matière de transparence varie d'une entreprise à l'autre. Si certaines entreprises se bornent à communiquer au ministère du commerce une description de leurs dispositions de protection de la vie privée dans le cadre de la procédure d'autocertification, la plupart publient ces dispositions sur leur site web, en plus de les télécharger sur le site du ministère. Toutefois, ces **dispositions ne sont pas toujours présentées sous une forme adaptée aux consommateurs et facile à lire**. Les hyperliens y renvoyant ne fonctionnent pas toujours correctement et ils ne pointent pas toujours vers les bonnes pages web.

---

20 http://www.export.gov/SafeHarbour/

21 https://SafeHarbour.export.gov/list.aspx

22 Le guide figure sur le site web consacré au programme, à l'adresse suivante: http://export.gov/SafeHarbour/ Helpful Hints: http://export.gov/SafeHarbour/eu/eg_main_018495.asp

Il ressort de la décision et de ses annexes que l'obligation faite aux entreprises de publier leurs dispositions en matière de protection de la vie privée **va au-delà d'une simple notification** de l'autocertification au ministère américain du commerce. Les exigences à remplir pour la certification, énoncées dans les questions souvent posées, incluent la communication d'une description de la politique de protection de la vie privée et d'informations transparentes quant au lieu où le texte de ces dispositions peut être consulté par le public[23]. Les déclarations concernant la politique de protection de la vie privée doivent être claires et facilement accessibles au public. Elles doivent comporter un hyperlien pointant vers le site web du ministère du commerce consacré à la sphère de sécurité qui dresse la liste de tous les adhérents dont la certification est «à jour», ainsi qu'un lien renvoyant à un prestataire chargé du règlement extrajudiciaire des litiges. Cependant, un certain nombre d'entreprises ayant adhéré au cadre entre 2000 et 2013 n'ont pas satisfait à ces exigences. Lors de contacts de travail avec la Commission en février 2013, le ministère du commerce a reconnu la possibilité que jusqu'à 10 % des entreprises certifiées n'aient, en réalité, pas publié sur leurs sites web respectifs une politique en matière de protection de la vie privée contenant une déclaration affirmative d'adhésion à la sphère de sécurité.

Des statistiques récentes font également ressortir l'existence d'un problème persistant, celui des **fausses déclarations d'adhésion à la sphère de sécurité**. Environ 10 % des entreprises affirmant avoir adhéré à la sphère de sécurité ne sont pas citées par le ministère du commerce parmi les adhérents dont la certification est à jour[24]. Ces fausses déclarations émanent à la fois d'entreprises n'ayant jamais adhéré au cadre de la sphère de sécurité et d'entreprises qui y ont adhéré par le passé mais ont ensuite omis d'envoyer tous les ans leur autocertification au ministère américain du commerce. Dans ce dernier cas, elles continuent de figurer sur le site web consacré à la sphère de sécurité mais le statut de leur certification n'est «plus à jour», ce qui signifie que ces entreprises ont adhéré au cadre et sont donc tenues de continuer à protéger les données déjà traitées. La commission fédérale du commerce est compétente pour intervenir dans les dossiers de pratiques frauduleuses et de non-respect des principes de la sphère de sécurité (voir le point 5.1). Le manque de clarté quant aux «fausses déclarations» nuit à la crédibilité du cadre.

Au cours des contacts réguliers qu'elle a entretenus avec lui en 2012 et 2013, la Commission européenne a averti le ministère du commerce que, pour remplir les obligations en matière de transparence, il ne suffisait pas que l'entreprise communique à ce ministère une description de sa politique de protection de la vie privée. Cette politique doit, en outre, être mise à la disposition du public. Le ministère du commerce a également été invité à **intensifier ses contrôles périodiques des sites web des entreprises**, censés succéder à la vérification effectuée dans le cadre de la première procédure d'autocertification ou de son renouvellement annuel, et à prendre des mesures à l'encontre des entreprises qui ne se conforment pas aux exigences en matière de transparence.

En guise de première réponse aux préoccupations de l'Union, **le ministère du commerce a rendue obligatoire, à partir de mars 2013,** la publication sur le site web public de toute entreprise adhérant à la sphère de sécurité - pour autant qu'elle possède un tel site - de sa politique de protection de la vie privée applicable aux données concernant les clients/utilisateurs. Dans le même temps, le ministère a commencé à avertir l'ensemble des

[23] Le 12 novembre 2013, le ministère du commerce a confirmé que: «Aujourd'hui, les entreprises qui possèdent un site web public et traitent des données relatives aux consommateurs/clients/visiteurs doivent faire figurer sur leurs sites web respectifs une politique de protection de la vie privée conforme aux principes de la sphère de sécurité (document: «U.S.-EU Cooperation to Implement the Safe Harbor Framework» du 12 novembre 2013).

[24] En septembre 2013, un cabinet de conseil australien, Galexia, a comparé les «fausses déclarations» d'adhésion à la sphère de sécurité pour les années 2008 et 2013. Son principal constat est que, parallèlement à une hausse du nombre d'adhérents au cadre entre 2008 et 2013 (de 1 109 à 3 246), le nombre de fausses déclarations est passé de 206 à 427 (http://www.galexia.com/public/about/news/about_news-id225.html).

entreprises dont les dispositions de protection de la vie privée ne comportaient pas déjà de lien renvoyant au site web du ministère consacré à la sphère de sécurité qu'elles devaient en ajouter un, afin de permettre aux consommateurs qui consultent le site de ces entreprises d'avoir directement accès à la liste et au site officiels relatifs à la sphère de sécurité. Cela permettra aux Européens dont les données sont traitées de vérifier immédiatement, sans avoir à chercher plus avant sur l'internet, les engagements qu'une entreprise a communiqués au ministère américain du commerce. En outre, le ministère a commencé à informer les entreprises que leurs dispositions de protection de la vie privée mises en ligne devaient mentionner les coordonnées de leur prestataire indépendant chargé du règlement des litiges[25].

Il convient d'accélérer ce processus pour garantir que toutes les entreprises certifiées se conforment pleinement aux exigences liées à la sphère de sécurité d'ici mars 2014 au plus tard (c'est-à-dire à l'échéance du renouvellement annuel de leur certification, à compter de l'instauration des nouvelles exigences en mars 2013).

Des inquiétudes subsistent toutefois quant à savoir si toutes les entreprises autocertifiées satisfont à l'intégralité des obligations en matière de transparence. Le ministère du commerce devrait procéder à des contrôles et à des enquêtes plus rigoureux pour vérifier le respect des engagements pris au moment de la première autocertification et de son renouvellement annuel.

4. L'INTEGRATION DES PRINCIPES DE LA SPHERE DE SECURITE RELATIFS A LA PROTECTION DE LA VIE PRIVEE DANS LES POLITIQUES DE PROTECTION DE LA VIE PRIVEE ADOPTEES PAR LES ENTREPRISES

Les entreprises autocertifiées doivent se conformer aux principes de protection de la vie privée figurant à l'annexe I de la décision pour obtenir et conserver les avantages de la sphère de sécurité.

Dans le rapport de 2004, la Commission constatait qu'un nombre important d'**entreprises n'avaient pas correctement intégré les principes de la sphère de sécurité relatifs à la protection de la vie privée** dans leurs politiques de traitement des données. Par exemple, les particuliers ne recevaient pas toujours une information claire et transparente sur les finalités des traitements des données les concernant ou n'avaient pas eu la possibilité de signifier leur refus dans l'hypothèse où leurs données devaient être divulguées à un tiers ou être utilisées à des fins incompatibles avec les finalités pour lesquelles elles avaient été initialement collectées. Dans ledit rapport, la Commission estimait que le ministère du commerce *«devrait être plus volontariste en ce qui concerne l'accès à la sphère de sécurité et la sensibilisation aux principes de celles-ci»*[26].

Les progrès accomplis à cet égard restent limités. Depuis le 1er janvier 2009, toute entreprise cherchant à renouveler son statut de certification pour la sphère de sécurité – ainsi qu'elle doit le faire annuellement – verra sa politique de protection de la vie privée évaluée préalablement par le ministère américain du commerce. Cette évaluation a toutefois une portée limitée. En effet, il n'existe **pas d'évaluation complète des pratiques effectives** dans les entreprises

[25] Entre mars et septembre 2013, le ministère du commerce a:
• informé les 101 entreprises *qui avaient déjà téléchargé leur politique de protection de la vie privée conforme aux principes de la sphère de sécurité sur le site correspondant du ministère* qu'elles devaient également faire figurer ces dispositions sur leur site web;
• informé les 154 entreprises qui ne l'avaient pas encore fait qu'elles devaient faire figurer dans leurs dispositions de protection de la vie privée un lien renvoyant vers le site consacré à la sphère de sécurité;
• informé plus de 600 entreprises qu'elles devaient indiquer, dans leurs dispositions de protection de la vie privée, les coordonnées de leur prestataire indépendant chargé du règlement des litiges.

[26] Voir la page 8 du rapport de 2004, SEC(2004) 1323.

autocertifiées, laquelle renforcerait pourtant sensiblement la crédibilité de la procédure d'autocertification.

Donnant suite aux appels de la Commission en faveur d'une surveillance plus rigoureuse et systématique des entreprises autocertifiées par le ministère américain du commerce, ce dernier accorde désormais **une plus grande attention aux nouvelles certifications**. Entre 2010 et 2013, le nombre de nouvelles certifications refusées et renvoyées aux entreprises, pour que celles-ci apportent des améliorations à leurs politiques de protection de la vie privée, a considérablement augmenté: il a doublé en ce qui concerne les entreprises sollicitant un renouvellement de leur certification et il a triplé en ce qui concerne les nouveaux adhérents à la sphère de sécurité[27]. Le ministère du commerce a assuré à la Commission que toute procédure de certification ou de renouvellement de celle-ci ne pouvait être achevée que si la politique de protection de la vie privée adoptée par l'entreprise remplissait toutes les exigences, ce qui signifie notamment que cette politique doit comporter un engagement d'adhésion aux principes de la sphère de sécurité relatifs à la protection de la vie privée et qu'elle doit être accessible au public. Toute entreprise est tenue de préciser, parmi les mentions devant figurer sur la liste des adhérents à la sphère de sécurité, l'endroit où la politique concernée est publiée. Elle doit aussi désigner clairement sur son site web un prestataire chargé du règlement extrajudiciaire des litiges et y faire figurer un lien renvoyant à la rubrique consacrée à l'autocertification pour la sphère de sécurité sur le site web du ministère américain du commerce. On estime toutefois que plus de 30 % des adhérents à la sphère de sécurité ne fournissent pas d'informations relatives au règlement des litiges dans le cadre de leur politique de protection de la vie privée figurant sur leur site web[28].

La majorité des entreprises que le ministère du commerce a radiées de la liste ont été exclues de la sphère de sécurité à la demande expresse des entreprises concernées (par exemple, les entreprises qui avaient fait l'objet d'une fusion ou d'une acquisition, avaient modifié leurs activités ou les avaient cessées). L'enregistrement d'un plus petit nombre d'entreprises disparues a été supprimé lorsqu'il a été constaté que leurs sites web respectifs mentionnés dans la liste n'étaient plus opérationnels et que leur certification revêtait le statut «plus à jour» depuis plusieurs années[29]. Il importe d'observer qu'aucun de ces retraits ne semble avoir eu lieu parce que la vérification effectuée par le ministère du commerce avait permis la détection de problèmes de conformité.

La liste des adhérents à la sphère de sécurité tient lieu d'avis public et d'enregistrement des engagements pris par toute entreprise qui y figure. **L'adhésion aux principes de la sphère de sécurité n'est pas limitée dans le temps** en ce qui concerne les données reçues au cours de la période pendant laquelle l'entreprise bénéficie des avantages de la sphère de sécurité; l'entreprise doit continuer à appliquer ces principes à ces données, tant qu'elle stocke, utilise ou communique celles-ci, et ce même si elle quitte la sphère de sécurité pour une raison quelconque.

---

27 Selon les statistiques qu'il a fournies en septembre 2013, le ministère du commerce a pris contact en 2010 avec 18 % (93) des 512 entreprises ayant envoyé leur première lettre ou déclaration d'autocertification et avec 16 % (231) des 1 417 entreprises ayant renouvelé leur certification, afin qu'elles apportent des améliorations à leur politique de protection de la vie privée et/ou à leur application des principes de la sphère de sécurité. Cependant, faisant suite aux demandes de la Commission tendant à ce que toutes les communications fassent l'objet de contrôles stricts, diligents et systématiques, le ministère a pris contact, à partir de la mi-septembre, avec 56 % (340) des 602 entreprises ayant envoyé leur première lettre ou déclaration d'autocertification et 27 % (493) des 1 809 entreprises ayant renouvelé leur certification, afin qu'elles apportent des améliorations à leur politique de protection de la vie privée.

28 Intervention de Chris Connolly (Galexia) devant la commission LIBE du Parlement européen le 7 octobre 2013.

29 À la date de décembre 2011, le ministère du commerce avait radié 323 entreprises de la liste des adhérents à la sphère de sécurité: 94 l'ont été parce qu'elles avaient cessé leurs activités, 88 parce qu'elles avaient fait l'objet d'une fusion ou d'une acquisition, 95 l'ont été à la demande de la société mère, 41 en raison d'un défaut persistant de renouvellement de leur certification et 5 pour des raisons diverses.

Les entreprises ayant demandé à adhérer à la sphère de sécurité mais dont la demande a été **rejetée au stade du contrôle administratif** effectué par le ministère du commerce et qui n'ont, de ce fait, jamais été ajoutées à liste des adhérents à la sphère de sécurité, se répartissent comme suit. **En 2010**, **6 %** (33) seulement des 513 entreprises ayant envoyé leur première certification n'ont jamais été inscrites sur cette liste au motif qu'elles ne satisfaisaient pas aux normes régissant l'autocertification établies par le ministère américain du commerce. **En 2013**, **12 %** (75) des 605 entreprises ayant adressé leur première certification n'ont jamais été inscrites sur la liste pour ce même motif.

Pour accroître la transparence des contrôles qu'il exerce, le ministère devrait au minimum dresser, sur son site web, la liste de toutes les entreprises qui ont été exclues de la sphère de sécurité, en indiquant les motifs du non-renouvellement de leur certification. Il conviendrait de ne plus considérer le statut «plus à jour» apparaissant sur la liste des adhérents à la sphère de sécurité comme une simple information: celui-ci devrait se doubler d'**un avertissement clair** – tant écrit que graphique — selon lequel l'entreprise correspondante ne remplit actuellement plus les exigences de la sphère de sécurité.

Par ailleurs, certaines entreprises n'ont toujours pas complètement intégré tous les principes de la sphère de sécurité. Outre le problème de transparence examiné ci-dessus au point 3, les politiques de protection de la vie privée appliquées par les entreprises autocertifiées manquent souvent de clarté en ce qui concerne les finalités des collectes de données et le droit de choisir, c'est-à-dire de consentir ou de s'opposer à la divulgation de données à un tiers. Le respect des principes de «notification» et de «choix» suscite, dès lors, des préoccupations. La notification et le choix sont, en effet, des éléments déterminants pour garantir que les personnes concernées conservent la maîtrise de ce qu'il advient des données à caractère personnel les concernant.

La première étape décisive du processus de mise en conformité, à savoir l'intégration des principes de la sphère de sécurité relatifs à la vie privée dans les politiques correspondantes des entreprises, est insuffisamment respectée. Le ministère du commerce devrait s'attaquer en priorité à cette question, en élaborant une méthodologie de mise en conformité à l'intention des entreprises, tant dans leurs pratiques de fonctionnement que dans les interactions avec leurs clients. **Il y a lieu que le ministère du commerce suive activement l'intégration des principes de la sphère de sécurité dans les politiques des entreprises en matière de protection de la vie privée** plutôt que de subordonner le contrôle de l'application desdits principes au dépôt de plaintes par des particuliers.

5. LE CONTROLE DE L'APPLICATION EXERCE PAR LES POUVOIRS PUBLICS

Plusieurs mécanismes existent pour assurer un contrôle effectif de l'application du cadre de la sphère de sécurité et pour offrir des voies de recours aux personnes victimes d'atteintes à la protection des données à caractère personnel les concernant, consécutives au non-respect des principes relatifs à la protection de la vie privée.

Conformément au principe d'application, les politiques de protection de la vie privée appliquées par les entreprises autocertifiées doivent comporter des mécanismes efficaces de contrôle du respect de ces principes. Selon le principe d'application tel qu'il est explicité par les FAQ 11, 5 et 6, cette obligation peut être remplie par une adhésion à des **instances ou organismes de recours indépendants** ayant déclaré publiquement leur compétence pour connaître des plaintes déposées par des particuliers pour manquement aux principes de la sphère de sécurité. Une autre façon de se conformer à cette obligation consiste, pour

l'entreprise, à s'engager à coopérer avec le **panel de l'UE sur la protection des données**[30]. En outre, les entreprises autocertifiées relèvent de la compétence de la commission fédérale du commerce en vertu de la section 5 du *Federal Trade Commission Act* (loi sur la Commission fédérale du commerce), qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce[31].

Dans son rapport de 2004, la Commission exprimait ses préoccupations quant à l'application du cadre de la sphère de sécurité et indiquait notamment que la commission fédérale du commerce devrait être plus volontariste en matière d'ouverture d'enquêtes et de sensibilisation des citoyens à leurs droits. Un autre sujet d'inquiétude tenait au manque de clarté en ce qui concerne la compétence de cette commission pour contrôler l'application des principes de la sphère de sécurité aux données sur les ressources humaines.

L'instance de recours chargée d'examiner les plaintes concernant ce type de données – à savoir le panel de l'UE sur la protection des données – n'a été saisie que d'une plainte[32]. Toutefois, la quasi-absence de plaintes ne permet pas de tirer de conclusion quant au fonctionnement optimal du cadre. Il conviendrait d'instaurer des contrôles d'office pour vérifier la mise en œuvre effective par les entreprises des engagements pris en matière de protection des données. Les autorités chargées de la protection des données dans les États membres de l'UE devraient également prendre des mesures pour faire connaître ce panel.

Des problèmes ont été mis en lumière dans le fonctionnement des instances et organismes de règlement extrajudiciaire des litiges en leur qualité d'organes de contrôle de l'application. Un certain nombre de ces organes ne disposent pas de moyens suffisants pour être en mesure de remédier aux cas de non-respect des principes de la sphère de sécurité. Il y a donc lieu de combler cette lacune.

5.1. La commission fédérale du commerce

La commission fédérale du commerce peut prendre des mesures répressives en cas de violation, par les entreprises, des engagements qu'elles ont pris à l'égard de la sphère de sécurité. Lorsque la sphère de sécurité a été instaurée, cette commission s'est engagée à examiner en priorité tous les dossiers déférés par les autorités des États membres de l'UE[33]. N'ayant reçu aucune plainte pendant les dix premières années d'application du cadre de la sphère de sécurité, la commission a décidé de rechercher les éventuelles infractions à ce dernier lors de chaque enquête qu'elle mènerait sur des atteintes à la vie privée et à la sécurité des données. Depuis 2009, la commission a poursuivi dix entreprises en justice pour violation de la sphère de sécurité. Ces actions ont notamment abouti à des ordonnances contenant des conventions de transaction – sous réserve du paiement de lourdes amendes – interdisant les fausses déclarations en matière de protection de la vie privée, y compris concernant le respect des principes de la sphère de sécurité, et imposant aux entreprises des programmes exhaustifs de protection de la vie privée ainsi que des audits pendant 20 ans. Les entreprises concernées

[30] Le panel de l'UE sur la protection des données est une entité compétente pour instruire et trancher les plaintes déposées par des particuliers pour violation alléguée des principes de la sphère de sécurité par une entreprise américaine adhérant à celle-ci. Les entreprises qui certifient respecter les principes de la sphère de sécurité doivent choisir d'adhérer à un mécanisme de recours indépendant ou de coopérer avec le panel de l'UE sur la protection des données pour remédier aux problèmes découlant du non-respect des principes de la sphère de sécurité. La coopération avec ce panel est néanmoins obligatoire lorsque l'entreprise américaine concernée traite des données à caractère personnel qui concernent des ressources humaines et sont transférées depuis l'Union dans le cadre d'une relation de travail. Si l'entreprise s'engage à coopérer avec le panel, elle doit également s'engager à suivre toute recommandation qu'il formulerait dans l'hypothèse où il estimerait qu'elle doit prendre des mesures spécifiques pour se conformer aux principes de la sphère de sécurité, y compris des mesures correctives ou compensatoires.

[31] Le ministère des transports exerce des compétences semblables à l'égard des transporteurs aériens, en vertu du titre 49 du United States Code (code de réglementations fédérales des États-Unis), article 41712.

[32] Cette plainte émanait d'un ressortissant suisse, de sorte que le panel l'a déférée à l'autorité suisse de protection des données (les États-Unis ont, en effet, établi un autre cadre de la sphère de sécurité pour la Suisse).

[33] Voir l'annexe V de la décision 2000/520/CE de la Commission du 26 juillet 2000.

doivent accepter de soumettre leur programme de protection de la vie privée à des évaluations indépendantes, à la demande de la commission fédérale du commerce. Ces évaluations sont communiquées régulièrement à cette dernière. Les ordonnances rendues par la commission fédérale du commerce interdisent également à ces entreprises de faire de fausses déclarations quant à leurs pratiques en matière de protection de la vie privée et à leur participation à la sphère de sécurité ou à des régimes similaires de protection de la vie privée. Ainsi en a décidé la commission fédérale du commerce, par exemple, à l'issue des enquêtes qu'elle avait menées sur Google, Facebook et Myspace[34]. En 2012, la société Google a, en effet, accepté de payer une amende de 22,5 millions d'USD pour mettre un terme à des allégations selon lesquelles elle aurait enfreint une ordonnance dont elle avait approuvé la teneur («consent order»). Dans toutes les enquêtes relatives à des atteintes alléguées à la vie privée, la commission fédérale du commerce examine d'office l'existence éventuelle d'une violation de la sphère de sécurité.

La commission fédérale du commerce a récemment réitéré ses déclarations et son engagement à examiner, en priorité, les dossiers déférés par les organismes d'autoréglementation et les États membres de l'UE portant sur des allégations de non-respect des principes de la sphère de sécurité[35]. Ces trois dernières années, elle n'a été saisie que de quelques dossiers émanant d'autorités européennes de protection des données.

La coopération transatlantique entre les autorités de protection des données a commencé à se développer au cours des derniers mois. Ainsi, le 26 juin 2013, la commission fédérale du commerce a signé avec l'autorité irlandaise de protection des données un protocole d'accord concernant l'entraide en matière de contrôle du respect des législations protégeant les données à caractère personnel dans le secteur privé. Ce protocole d'accord établit un cadre pour intensifier, rationaliser et rendre plus efficace la coopération en matière de contrôle du respect de la protection de la vie privée[36].

En août 2013, la commission fédérale du commerce a annoncé un renforcement des vérifications auxquelles sont soumises les entreprises exerçant un contrôle sur d'importantes bases de données à caractère personnel. Elle a également créé un portail sur lequel les consommateurs peuvent porter plainte contre une entreprise américaine pour atteinte à la vie privée[37].

La commission fédérale du commerce devrait également redoubler d'efforts pour instruire les dossiers relatifs aux fausses déclarations d'adhésion à la sphère de sécurité. En effet, une entreprise qui affirme sur son site web se conformer aux exigences de la sphère de sécurité mais ne figure pas sur la liste du ministère du commerce parmi les adhérents dont la certification est «à jour» trompe les consommateurs et abuse de leur confiance. Les fausses déclarations affaiblissent la crédibilité du système dans son ensemble et, par conséquent, doivent être immédiatement retirées du site web de chaque entreprise contrevenante. Ces dernières devraient être liées par l'obligation opposable de ne pas tromper les consommateurs.

---

34 Entre 2009 et 2012, la commission fédérale du commerce a clôturé dix actions relatives à des violations d'engagements au titre de la sphère de sécurité: FTC c. Javian Karnani, et Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Voir: «Federal Trade Commission of Safe Harbour Commitments»: http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf Voir également: «Case Highlights»: http://business.ftc.gov/us-eu-Safe-Harbour-framework La plupart de ces litiges concernaient des entreprises qui avaient adhéré à la sphère de sécurité puis avaient continué de déclarer qu'elles en étaient adhérentes mais sans avoir renouvelé leur certification annuelle.

35 M[me] Julie Brill, membre de la commission fédérale du commerce, a réitéré cet engagement lors d'une réunion avec les autorités européennes de protection des données (représentées au sein du groupe de travail de l'article 29) tenue le 17 avril 2013 à Bruxelles.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Les consommateurs aux États-Unis peuvent déposer leur plainte sur le portail créé à cet effet par la commission fédérale du commerce (https://www.ftccomplaintassistant.gov/) et les consommateurs étrangers peuvent porter plainte via le site econsumer.gov (http://www.econsumer.gov).

La commission fédérale du commerce devrait continuer à détecter les fausses déclarations d'adhésion à la sphère de sécurité, comme dans l'affaire *Karnani* où elle a imposé la fermeture d'un site web créé et exploité par des entreprises établies en Californie qui se prévalaient abusivement d'une telle adhésion et se livraient à des pratiques frauduleuses de commerce électronique ciblant les consommateurs européens[38].

Le 29 octobre 2013, la commission a annoncé qu'elle avait ouvert «de nombreuses enquêtes concernant le respect de la sphère de sécurité au cours des derniers mois» et que davantage d'actions sur ce front «pouvaient être attendues dans les mois à venir». Elle a également confirmé qu'elle était «résolue à chercher des moyens d'améliorer son efficacité» et «continuera[it] à accueillir favorablement toute piste concrète, comme la plainte reçue le mois [précédent], émanant d'un défenseur des droits des consommateurs établi en Europe, alléguant de nombreuses violations liées à la sphère de sécurité»[39]. Elle s'est, en outre, engagée à «contrôler systématiquement le respect des ordonnances relatives à la sphère de sécurité, comme c'est le cas de toutes [ses] ordonnances»[40].

Le 12 novembre 2013, la commission fédérale du commerce a informé la Commission européenne que, «**si la politique de protection de la vie privée d'une entreprise promet des protections conformes à la sphère de sécurité, l'omission par cette entreprise de s'enregistrer ou de renouveler son enregistrement n'est pas, en soi, de nature à soustraire cette entreprise au contrôle du respect, par la FTC, de ces engagements au titre de la sphère de sécurité**»[41].

En novembre 2013, le ministère du commerce a informé la Commission européenne que pour «faire en sorte que les entreprises ne fassent pas de "fausses déclarations" de participation à la sphère de sécurité, il entamerait des démarches auprès des adhérents à la sphère de sécurité un mois avant la date de renouvellement de leur certification, pour leur décrire les étapes à suivre dans l'hypothèse où ils décideraient de ne pas procéder à ce renouvellement». **Le ministère du commerce «intimera aux entreprises** de cette catégorie de faire disparaître toutes les références à une participation à la sphère de sécurité, y compris toute utilisation de la marque de certification correspondante, de leur politique de protection de la vie privée et de leur site web, et il **les avertira clairement que tout manquement à cet égard est passible de poursuites par la FTC**»[42].

Pour lutter contre le phénomène des fausses déclarations d'adhésion à la sphère de sécurité, les politiques de protection de la vie privée affichées par les entreprises autocertifiées sur leur site web devraient toujours comporter un lien pointant vers le site web du ministère du commerce consacré à la sphère de sécurité où sont nommés tous les adhérents dont la certification est «à jour». Les Européens dont les données sont traitées pourront ainsi vérifier immédiatement, sans autres recherches, si la certification d'une entreprise ayant adhéré à la sphère de sécurité est à jour. En mars 2013, le ministère du commerce a commencé à imposer cette exigence aux entreprises mais il conviendrait qu'il intensifie ce processus.

Une priorité essentielle pour assurer le fonctionnement correct et effectif du cadre – outre les mesures prises par le ministère américain décrites ci-dessus – est le suivi permanent assuré par la commission fédérale du commerce et le contrôle consécutif de l'application effective des principes de la sphère de sécurité. Il y a lieu, en particulier, d'augmenter le nombre de

---

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf et http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Lettre de la présidente de la commission fédérale du commerce, Edith Ramirez, à la vice-présidente de la Commission européenne, Viviane Reding.

41 Lettre de la présidente de la commission fédérale du commerce, Edith Ramirez, à la vice-présidente de la Commission européenne, Viviane Reding.

42 Document «U.S.-EU Cooperation to Implement the Safe Harbor Framework» du 12 novembre 2013.

vérifications et d'enquêtes menées d'office pour s'assurer du respect, par les entreprises, des principes de la sphère de sécurité. Il conviendrait également de faciliter davantage le dépôt des plaintes auprès de la commission fédérale du commerce.

5.2. Le panel de l'UE sur la protection des données

Le panel de l'UE sur la protection des données est une entité créée en vertu de la décision relative à la sphère de sécurité. Il est compétent pour instruire les plaintes de particuliers concernant des données à caractère personnel recueillies dans le contexte d'une relation de travail et pour connaître des affaires relatives à des entreprises certifiées qui l'ont désigné pour le règlement de leurs litiges survenant dans le cadre de la sphère de sécurité (53 % de l'ensemble des entreprises). Il est composé de représentants de différentes autorités chargées de la protection des données dans l'UE.

À ce jour, il a été saisi de quatre plaintes (deux en 2010 et deux en 2013). En 2010, il a déféré deux plaintes à des autorités nationales de protection des données (Royaume-Uni et Suisse). Les troisième et quatrième plaintes sont actuellement en cours d'examen. Ce modeste nombre de plaintes tient tout d'abord au fait que les pouvoirs du panel sont essentiellement limités à certains types de données, comme indiqué ci-dessus.

Ensuite, le faible volume de dossiers dont le panel est saisi pourrait s'expliquer en partie par la méconnaissance de l'existence de cette entité. Depuis 2004, la Commission européenne donne une plus grande visibilité sur son site web aux informations concernant le panel[43].

Pour qu'un meilleur usage soit fait du panel, les entreprises établies aux États-Unis qui ont choisi de coopérer avec lui et de se conformer à ses décisions, pour l'ensemble ou certaines des catégories de données à caractère personnel couvertes par leurs autocertifications respectives, devraient indiquer clairement et visiblement dans leurs engagements au titre de leur politique de protection de la vie privée qu'elles autorisent le ministère du commerce à contrôler cet aspect. Une page spéciale devrait être consacrée, sur le site web de chacune des autorités européennes de protection des données, à la sphère de sécurité afin de la faire mieux connaître en Europe auprès des entreprises et des personnes dont les données sont traitées.

5.3. Amélioration du contrôle de l'application

Les lacunes décrites ci-dessus en matière de transparence et de contrôle de l'application préoccupent les entreprises européennes quant à l'incidence négative que peut avoir le cadre de la sphère de sécurité sur leur compétitivité. Lorsqu'une entreprise européenne est en concurrence avec une entreprise américaine qui exerce ses activités dans le cadre de la sphère de sécurité mais qui, dans la pratique, n'en applique pas les principes, elle se trouve dans une position concurrentielle désavantageuse par rapport à sa concurrente américaine.

Par ailleurs, la compétence de la commission fédérale du commerce englobe les manœuvres et les pratiques déloyales ou frauduleuses «dans le domaine du commerce». La section 5 du *Federal Trade Commission Act* (loi sur la Commission fédérale du commerce) prévoit des exceptions à cette compétence en ce qui concerne, entre autres, les **télécommunications**. Ne relevant pas du champ d'action de la commission fédérale du commerce, les entreprises de télécommunications ne sont pas autorisées à adhérer à la sphère de sécurité. Or, étant donné la convergence croissante des technologies et des services, nombreux sont leurs

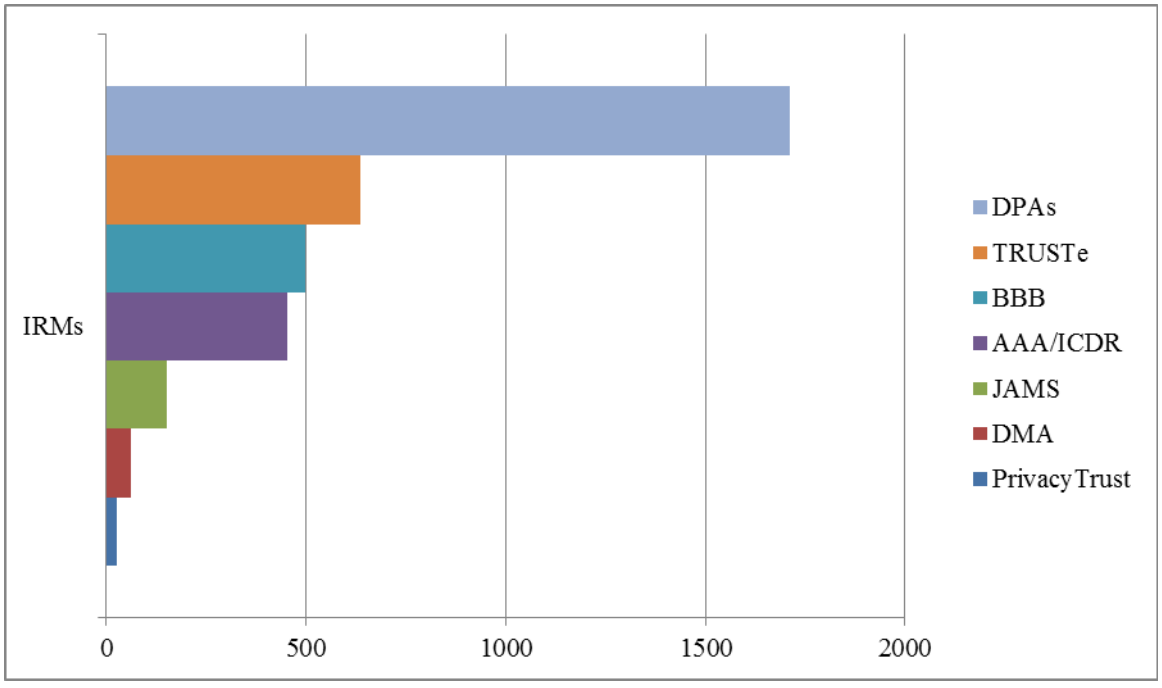
[43] Conformément au rapport de 2004, un avis d'information a été publié, sous la forme de questions et réponses rédigées par le panel de l'UE sur la protection des données, sur un site web de la Commission (celui de la direction générale de la justice) dans le but de sensibiliser les citoyens et de les aider à porter plainte s'ils estiment que des données à caractère personnel les concernant ont été traitées en violation des principes de la sphère de sécurité: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_fr.pdf
Le formulaire de plainte type est disponible à l'adresse suivante:http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/files/ussh/complaint_form_20130206_fr.pdf

concurrents directs dans le secteur américain des TIC qui adhèrent à la sphère de sécurité. L'exclusion des entreprises de télécommunications des échanges de données dans le cadre de la sphère de sécurité inquiète certains opérateurs de télécommunications européens. Selon l'Association européenne des exploitants de réseaux de télécommunications (ETNO), «cette situation va manifestement à l'encontre de la plus importante demande des opérateurs de télécommunications concernant la nécessité de garantir des conditions égales pour tous»[44].

6. LE RENFORCEMENT DES PRINCIPES DE LA SPHERE DE SECURITE RELATIFS A LA PROTECTION DE LA VIE PRIVEE

6.1. Règlement extrajudiciaire des litiges

Le principe d'application exige la mise en place de «**mécanismes de recours [...] facilement accessibles et abordables économiquement** permettant d'étudier tous les litiges et les plaintes déposés par des particuliers». À cet effet, le régime de la sphère de sécurité instaure un système de règlement extrajudiciaire des litiges (REL) par un tiers indépendant[45], afin de fournir des solutions rapides aux particuliers. Les trois principales entités dotées de mécanismes de recours sont le panel de l'UE sur la protection des données, les bureaux d'éthique commerciale et TRUSTe.



44 Les «Considérations de l'ETNO» reçues le 4 octobre 2013 par les services de la Commission abordent également 1) la définition des données à caractère personnel dans le cadre de la sphère de sécurité; 2) le suivi insuffisant de la sphère de sécurité; 3) et le fait que les «entreprises américaines peuvent transférer des données moyennant de bien moins nombreuses restrictions que celles qui s'appliquent à leurs homologues européennes», ce qui «constitue une discrimination patente à l'égard des entreprises européennes et affecte la compétitivité de celles-ci». En vertu des règles de la sphère de sécurité, pour divulguer des informations à un tiers, les organisations sont tenues d'appliquer les principes de notification et de choix. Les organisations qui le souhaitent peuvent transférer des informations à un tiers agissant en qualité de mandataire si elles certifient auparavant que le tiers souscrit aux principes de la sphère de sécurité ou est soumis aux dispositions de la directive ou d'un autre mécanisme attestant le niveau adéquat de la protection ou encore si elle passe un accord écrit avec ce tiers dans lequel celui-ci s'engage à assurer au moins le même niveau de protection que les principes.

45 La directive de l'UE 2013/11/UE sur le règlement extrajudiciaire des litiges de consommation souligne l'importance de disposer de procédures de règlement extrajudiciaire des litiges indépendantes, impartiales, transparentes, efficaces, rapides et équitables.

Le recours au REL a augmenté depuis 2004 et le ministère du commerce a renforcé le contrôle des prestataires de REL américains, afin de garantir qu'ils exposent des informations claires, accessibles et compréhensibles en ce qui concerne la procédure de recours. L'efficacité de ce système reste néanmoins à démontrer en raison du nombre restreint de cas traités à ce jour[46].

Bien que le ministère du commerce soit parvenu à réduire les redevances demandées par les prestataires de REL, deux des sept plus grands prestataires dans ce domaine continuent à imposer des redevances aux particuliers qui portent plainte[47]. Il s'agit des prestataires de REL auxquels s'adressent environ 20 % des entreprises adhérentes à la sphère de sécurité. Ces sociétés ont sélectionné un prestataire de REL qui réclame une redevance aux clients qui portent plainte. Or ces pratiques ne sont pas conformes au principe d'application de la sphère de sécurité qui ouvre aux particuliers le droit d'accéder à un «mécanisme de recours indépendant facilement accessible et abordable économiquement». Au sein de l'Union européenne, l'accès à un service de règlement des litiges indépendant, fourni par le panel de l'UE sur la protection des données, est gratuit pour toutes les personnes concernées.

Le 12 novembre 2013, le ministère du commerce confirmait qu'il «continuerait à défendre le droit des citoyens de l'UE à la vie privée et qu'il étudierait avec les prestataires de REL les possibilités de réduire davantage leurs redevances».

En ce qui concerne les sanctions, les prestataires de REL ne possèdent pas tous les outils nécessaires pour remédier aux manquements aux principes de protection de la vie privée. En outre, la publication des constatations de non-respect de ces principes ne semble pas être envisagée parmi l'éventail des sanctions et mesures applicables par l'ensemble des prestataires de REL.

Les prestataires de REL sont également invités à déférer à la commission fédérale du commerce les affaires concernant les entreprises qui ne se conforment pas aux conclusions de la procédure de REL, ou rejettent la décision des prestataires de REL, afin que ladite commission puisse procéder à un examen et à une enquête et, le cas échéant, prendre des mesures répressives. Néanmoins, à ce jour, les prestataires de REL n'ont pas encore déféré d'affaires à la commission fédérale du commerce[48].

Les prestataires de règlement extrajudiciaire des litiges tiennent, sur leur site, des listes d'entreprises (participants REL) qui font appel à leurs services. Cela permet aux consommateurs de vérifier aisément si, en cas de litige avec une entreprise, un particulier peut déposer une plainte auprès d'un prestataire de REL donné. Ainsi, par exemple, le prestataire

---

[46] À titre d'exemple, un important prestataires de services («TRUSTe») a indiqué qu'il avait été saisi de 881 demandes en 2010, mais que seules trois d'entre elles avaient été jugées recevables et fondées, justifiant que l'entreprise concernée soit invitée à changer sa politique de protection de la vie privée et son site web. En 2011, le nombre de plaintes s'est élevé à 879 et, dans un cas, l'entreprise a été invitée à modifier sa politique de protection de la vie privée. En ce qui concerne le ministère américain du commerce, la plupart des plaintes dans le cadre du REL émanent de consommateurs, par exemple, des utilisateurs qui avaient oublié leur mot de passe et ne pouvaient pas le récupérer auprès du service internet. À la demande de la Commission, le ministère du commerce a développé de nouveaux critères de communication de statistiques à utiliser pour l'ensemble des REL. Ces critères établissent une distinction entre les simples demandes, d'une part, et les plaintes, d'autre part, et fournissent des éclaircissements supplémentaires concernant les types de plaintes reçues. Ces nouveaux critères doivent cependant faire l'objet d'un débat plus approfondi qui permettra d'assurer que les nouvelles statistiques en 2014 concerneront l'ensemble des prestataires de REL, qu'elles seront comparables et fourniront des informations déterminantes pour évaluer le caractère effectif du mécanisme de recours.

[47] L'International Centre for Dispute Resolution/l'American Arbitration Association (ICDR/AAA) et JAMS réclament, respectivement, 200 USD et 250 USD pour «frais de dossier». Le ministère du commerce a informé la Commission qu'il avait travaillé avec AAA, le prestataire de règlement de litiges pour particuliers le plus onéreux, afin de concevoir un programme propre à la sphère de sécurité, pour réduire le coût pesant sur les consommateurs de plusieurs milliers de dollars à un taux forfaitaire de 200 USD.

[48] Voir FAQ 11.

de REL, le bureau d'éthique commerciale, dresse la liste de l'ensemble des entreprises relevant du système de règlement extrajudiciaire des litiges de son bureau. De nombreuses entreprises prétendent néanmoins relever d'un système spécifique de règlement des litiges alors que les prestataires de REL ne les désignent pas comme des participantes à leur régime de règlement de litiges[49].

Les mécanismes de REL doivent être aisément accessibles, indépendants et économiquement abordables pour les particuliers. Une personne concernée devrait pouvoir déposer une plainte sans avoir à subir des contraintes excessives. Tous les organismes de REL devraient publier sur leur site web des statistiques sur les plaintes déposées et traitées ainsi que des informations spécifiques concernant leur issue. Enfin, les organismes de REL devraient être soumis à un contrôle ultérieur visant à garantir que les informations qu'ils fournissent au sujet de la procédure et des modalités de dépôt de plaintes sont claires et intelligibles, de manière à faire du règlement des litiges un mécanisme effectif, fiable et porteur de résultats. Il convient également de répéter que la publication des constatations de non-conformité devrait figurer parmi les sanctions obligatoires des REL.

6.2. Transfert ultérieur

La croissance exponentielle des flux de données impose de garantir la protection continue des données à caractère personnel à toutes les étapes de leur traitement, notamment lorsqu'une entreprise ayant souscrit à la sphère de sécurité transfère ces données à **un tiers responsable du traitement**. En conséquence, la nécessité de faire mieux respecter la sphère de sécurité concerne non seulement les adhérents à la sphère de sécurité mais aussi les sous-traitants.

Le régime de la sphère de sécurité permet les transferts ultérieurs à un tiers agissant en qualité de «mandataire» si l'entreprise adhérente à la sphère de sécurité «certifie auparavant que le tiers souscrit aux principes de la "sphère de sécurité" ou est soumis aux dispositions de la directive ou d'un autre mécanisme attestant le niveau adéquat de la protection ou encore si elle passe un accord écrit avec ce tiers dans lequel celui-ci s'engage à assurer au moins le même niveau de protection que les principes»[50]. Par exemple un fournisseur de services informatiques en nuage est invité par le ministère du commerce à conclure un contrat même s'il est «respectueux de la sphère de sécurité» et reçoit des données à caractère personnel en vue de leur traitement[51]. Néanmoins, cette disposition n'est pas claire dans l'annexe II de la décision relative à la sphère de sécurité.

Le recours aux sous-traitants ayant considérablement augmenté au cours des dernières années, en particulier dans le contexte de l'informatique en nuage, lorsqu'un tel contrat est conclu, une entreprise faisant partie de la sphère de sécurité devrait en informer le ministère du commerce et être tenue de rendre publiques les garanties concernant la vie privée[52].

---

49 Exemples: Amazon a informé le ministère du commerce qu'il avait recours au bureau d'éthique commerciale en tant que prestataire de REL. Or ce dernier ne mentionne pas Amazon parmi les participants à son système de REL. À l'inverse, Arsalon Technologies (www.arsalon.net), un prestataire de services de stockage dans le nuage, figure sur la liste de REL du bureau d'éthique commerciale au titre de la sphère de sécurité, mais la certification de cette entreprise n'est pas à jour (situation au 1er octobre 2013). Les bureaux d'éthique commerciale, TRUSTe et d'autres prestataires de REL doivent retirer ou corriger les déclarations de certification erronées. Ils devraient être liés par une obligation opposable de ne certifier que les entreprises qui ont adhéré à la sphère de sécurité.

50 Voir Décision 2000/520/CE de la Commission page 7 (transfert ultérieur).

51 Voir: «Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing»: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

52 Ces remarques concernent les prestataires de services qui ne font pas partie de la sphère de sécurité. Selon le cabinet de Conseil Galexia consultancy, «le niveau d'adhésion (et de conformité) à la sphère de sécurité parmi les prestataires de services d'informatique en nuage est très élevé. Ces prestataires ont généralement plusieurs niveaux de protection de la vie privée, combinant souvent des contrats directs avec les clients et des dispositions globales en matière de protection de la vie privée. À une ou deux importantes exceptions près, les fournisseurs de services d'informatique en nuage dans le cadre de la sphère de sécurité respectent les dispositions clés concernant le règlement des litiges et la mise en œuvre. Il ne figure, à l'heure actuelle,

Les trois éléments précités, à savoir le mécanisme de règlement extrajudiciaire des litiges, une supervision renforcée et les transferts ultérieurs de données, devraient être précisés davantage.

7. L'ACCES AUX DONNEES TRANSFEREES DANS LE CADRE DU REGIME DE LA SPHERE DE SECURITE

Dans le courant de l'année 2013, des informations sur l'ampleur et la portée des programmes de surveillance des États-Unis ont suscité des préoccupations concernant la continuité de la protection des données à caractère personnel légalement transférées aux États-Unis au titre de la sphère de sécurité. Par exemple, toutes les entreprises participant au programme PRISM, qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États-Unis, semblent être certifiées dans le cadre de la sphère de sécurité. La sphère de sécurité est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'UE.

La décision relative à la sphère de sécurité prévoit, à son annexe I, que l'adhésion aux principes peut être limitée par les exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États-Unis ou par les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles. Pour être valides, les limitations et restrictions à la jouissance des droits fondamentaux doivent être interprétées restrictivement; elles doivent être énoncées dans une législation accessible au public et être nécessaires et proportionnées dans une société démocratique. En particulier, la décision relative à la sphère de sécurité précise que ces limitations ne sont permises que **dans la mesure nécessaire** aux exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois[53]. Alors que le traitement exceptionnel de données pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois est prévu dans le régime de la sphère de sécurité, l'accès à grande échelle des agences de renseignement aux données transférées aux États-Unis dans le cadre des transactions commerciales n'était pas prévisible lorsque la sphère de sécurité a été adoptée.

En outre, pour des raisons de transparence et de sécurité juridique, la Commission européenne devrait être informée par le ministère du commerce de tout texte législatif ou règlement du gouvernement qui affecterait l'adhésion aux principes de la sphère de sécurité[54]. Le recours aux dérogations devrait être soigneusement contrôlé et celles-ci ne devraient pas être utilisées d'une manière qui entamerait la protection accordée par les **principes**[55]. Plus précisément, l'accès à grande échelle des autorités américaines aux données traitées par les entreprises autocertifiées au titre de la sphère de sécurité risque de porter atteinte à la confidentialité des communications électroniques.

---

aucun prestataire de services d'informatique en nuage dans la liste des entreprises ayant fait de fausses déclarations d'adhésion.» (intervention de Chris Connolly, de Galexia, lors de l'audience publique consacrée à une enquête de la commission LIBE du Parlement européen sur la surveillance de masse électronique des citoyens de l'Union»).

53 Voir l'annexe I de la décision relative à la sphère de sécurité. «L'adhésion aux principes peut être limitée par: a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; ou c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables. Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations doivent s'efforcer d'appliquer ces principes de manière complète et transparente, y compris en indiquant - dans leurs codes de protection de la vie privée - dans quels domaines les exceptions visées au point b) ci-dessus s'appliqueront de façon régulière. Pour la même raison, lorsque les principes et/ou les lois des États-Unis permettent aux organisations de faire un choix, celles-ci sont invitées à opter, dans la mesure du possible, pour le niveau de protection le plus élevé».

54 Avis n°4/2000 sur le niveau de protection assuré par les «principes de la sphère de sécurité» adopté, le 16 mai 2000, par le groupe de travail «Article 29».

55 Avis n°4/2000 sur le niveau de protection assuré par les «principes de la sphère de sécurité» adopté, le 16 mai 2000, par le groupe de travail «Article 29».

7.1. Proportionnalité et nécessité

Il ressort des conclusions du groupe de travail qu'un certain nombre de bases juridiques prévues par la législation américaine permettent la collecte et le traitement à grande échelle des données à caractère personnel stockées ou traitée par des sociétés établies aux États-Unis. Cela peut recouvrir des données précédemment transférées de l'UE vers les États-Unis dans le cadre de la sphère de sécurité, ce qui soulève la question du respect ininterrompu des principes de la sphère de sécurité. Ces programmes étant à grande échelle, il est possible que les données transférées dans le cadre de la sphère de sécurité soient accessibles aux autorités américaines et traitées par celles-ci au-delà de ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale, comme le prévoit l'exception énoncée dans la décision relative à la sphère de sécurité.

7.2. Limitations et voies de droit

Il ressort des conclusions du groupe de travail que ce sont principalement les ressortissants des États-Unis et les personnes qui y résident légalement qui bénéficient des garanties prévues en droit américain. Il n'existe, en outre, aucune possibilité, que ce soit pour les personnes concernées de l'UE ou des États-Unis, d'obtenir l'accès, la rectification ou la suppression de données ou d'exercer des voies de droit administratives ou judiciaires si, dans le cadre des programmes de surveillance des États-Unis, des données à caractère personnel les concernant sont collectées et traitées ultérieurement.

7.3. Transparence

Les entreprises n'indiquent pas systématiquement, dans leurs dispositions de protection de la vie privée, à quel moment elles dérogent aux principes. Les particuliers et les entreprises n'ont donc pas connaissance de l'usage qui est fait des données les concernant. Cela est particulièrement pertinent pour ce qui est de l'exploitation des programmes de surveillance américains en question. Il s'ensuit que les Européens dont les données sont transférées à une entreprise aux États-Unis qui a adhéré à la sphère de sécurité peuvent ne pas être informés par cette entreprise que l'accès aux données les concernant est possible[56]. Cela soulève la question du respect des principes de la sphère de sécurité sur la transparence. Il conviendrait d'assurer la transparence dans la plus grande mesure possible, sans mettre en péril la sécurité nationale. En plus de devoir, comme cela est actuellement prévu, indiquer dans leurs dispositions de protection de la vie privée les cas où ces principes peuvent être limités par les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles, les entreprises devraient aussi être encouragées à indiquer, dans ces mêmes dispositions, les situations dans lesquelles elles dérogent aux principes pour répondre à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois.

8. CONCLUSIONS ET RECOMMANDATIONS

Depuis qu'elle a été adoptée en 2000, la sphère de sécurité est devenue un vecteur pour les flux de données à caractère personnel entre l'Union européenne et les États-Unis. L'importance de disposer d'une protection efficace en cas de transferts de données à caractère personnel a augmenté du fait de la croissance exponentielle des flux de données, cruciales pour l'économie numérique, et des grandes évolutions en matière de collecte, de traitement et

[56] Des informations relativement transparentes à cet égard sont fournies par certaines entreprises européennes adhérentes à la sphère de sécurité. Nokia, par exemple, qui est établie aux États-Unis et souscrit à la sphère de sécurité, fournit l'information suivante sur sa politique de protection de la vie privée. *«Nous pourrions être légalement tenus de divulguer des données à caractère personnel vous concernant à certaines autorités ou à d'autres tiers, par exemple, à des agences répressives, dans les pays où nous sommes présents ou bien dans lesquels des tiers agissant en notre nom sont présents.»*

d'utilisation des données. Les sociétés du web, telles que Google, Facebook, Microsoft, Apple et Yahoo, ont des centaines de millions de clients en Europe, et elles transfèrent des données à caractère personnel destinées à être traitées aux États-Unis à une échelle qui était inconcevable en l'an 2000, lors de la création de la sphère de sécurité.

Les lacunes qui affectent la transparence et l'exécution de l'accord contribuent à perpétuer des problèmes spécifiques qui doivent être résolus:

a) transparence des dispositions de protection de la vie privée adoptées par les adhérents à la sphère de sécurité,

b) mise en œuvre effective des principes relatifs à la protection de la vie privée par les entreprises établies aux États-Unis, et

c) caractère effectif du contrôle de l'application desdits principes.

Par ailleurs, l'**accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis** soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis.

Eu égard à ces considérations, la Commission juge utile de formuler les **recommandations** suivantes:

Transparence

1. *Les entreprises autocertifiées devraient rendre publiques leurs dispositions de protection de la vie privée*. Il ne suffit pas qu'elles fournissent au ministère du commerce une description de leurs *dispositions* de protection de la vie privée. Ces dernières devraient être consultables par le public sur les sites web respectifs des entreprises, et formulées de manière claire et intelligible.

2. *Les dispositions de protection de la vie privée rendues publiques sur les sites web respectifs des entreprises autocertifiées devraient toujours inclure un lien pointant vers le site web du ministère du commerce consacré à la sphère de sécurité, qui dresse la liste de l'ensemble des adhérents au cadre dont la certification est à jour*. Les Européens dont les données sont traitées pourront ainsi vérifier immédiatement, sans autres recherches, si la certification d'une entreprise ayant adhéré à la sphère de sécurité est à jour. La crédibilité du régime s'en trouverait améliorée grâce à la diminution des possibilités de fausses déclarations d'adhésion à la sphère de sécurité. Le ministère du commerce a commencé à imposer cette exigence aux entreprises en mars 2013, mais il conviendrait qu'il intensifie ce processus.

3. *Les entreprises autocertifiées devraient publier les conditions de protection de la vie privée figurant dans tout contrat conclu entre elles et leurs sous-traitants, par exemple, pour les services d'informatique en nuage*. La sphère de sécurité autorise la poursuite des transferts depuis les entreprises certifiées adhérentes à la sphère de sécurité à des tiers agissant en tant que mandataires, par exemple, à des fournisseurs de services en nuage. Il nous semble que, dans ces cas, le ministère du commerce exige des entreprises autocertifiées qu'elles concluent un contrat. Néanmoins, lors de la conclusion d'un tel contrat, une entreprise adhérente à la sphère de sécurité devrait également en aviser le ministère du commerce et être tenue de rendre publiques les garanties concernant la protection de la vie privée.

4. *Signalement clair sur le site web du ministère du commerce de toutes les entreprises dont la certification n'est plus à jour.* La marque de certification «plus à jour» dans la liste des membres de la sphère de sécurité dressée par le ministère du commerce devrait s'accompagner d'un avertissement clair selon lequel l'entreprise correspondante ne remplit actuellement plus les exigences de la sphère de sécurité. Néanmoins, lorsque le statut d'une certification n'est «plus à jour», l'entreprise concernée est tenue de continuer à appliquer les exigences relatives à la sphère de sécurité aux données qu'elle a reçues lorsque sa certification était encore «à jour».

Recours

5. *Les dispositions de protection de la vie privée mises sur les sites web des entreprises doivent inclure un lien dirigeant vers le site d'un prestataire de règlement extrajudiciaire des litiges (REL) et/ou du panel de l'UE sur la protection des données.* Cela permettra aux Européens dont les données sont traitées de prendre immédiatement contact, en cas de problème, avec le prestataire de REL ou le panel de l'UE sur la protection des données. En mars 2013, le ministère du commerce a commencé à imposer cette exigence aux entreprises, mais il conviendrait d'intensifier ce processus.
6. *Le REL devrait être facilement accessible et abordable économiquement*. Certains organismes prestataires de REL ayant adhéré à la sphère de sécurité continuent à facturer des redevances aux particuliers - dont les montants peuvent être très élevés pour un utilisateur donné - pour le traitement de leur plainte (200 à 250 USD). En Europe, en revanche, la législation prévoit l'accès gratuit des citoyens au panel de l'UE sur la protection des données, en ce qui concerne les plaintes déposées au titre de la sphère de sécurité.

7. *Le ministère du commerce devrait contrôler plus systématiquement les prestataires de REL sous l'angle de la transparence et de l'accessibilité des informations qu'ils fournissent à propos de la procédure utilisée et du suivi accordé aux plaintes.* Cela fait du règlement des litiges un mécanisme effectif et fiable, porteur de résultats. De même, répétons que la publication des constatations de non-conformité devrait également figurer parmi les sanctions obligatoires des REL.

Mise en œuvre

8. *À la suite d'une certification ou d'un renouvellement de la certification d'entreprises au titre de la sphère de sécurité, un certain pourcentage d'entre elles devraient être soumises à des enquêtes d'office concernant le respect effectif de leurs dispositions de protection de la vie privée (allant au-delà du contrôle du respect des exigences formelles).*

9. *Toutes les fois où une non-conformité est constatée, à l'issue d'une plainte ou d'une enquête, l'entreprise concernée devrait, après un an, faire l'objet d'une enquête de suivi spécifique.*

10. *En cas de doutes au sujet de la conformité d'une entreprise ou si des plaintes sont en cours d'examen, le ministère du commerce devrait en informer l'autorité compétente chargée de la protection des données dans l'État membre de l'UE concerné.*

11. *Les fausses déclarations d'adhésion à la sphère de sécurité devraient continuer à être examinées.* Une entreprise qui déclare, sur son site web, se conformer aux exigences de la sphère de sécurité mais ne figure pas sur la liste du ministère du commerce parmi les adhérents dont la certification est à jour trompe ses clients et abuse de leur confiance. Les fausses déclarations affaiblissent la crédibilité du système dans son ensemble et devraient, dès lors, être immédiatement retirées du site web de chaque entreprise contrevenante.

Accès par les autorités des États-Unis

12. *Les politiques de protection de la vie privée adoptées par les entreprises autocertifiées doivent comporter des informations sur la mesure dans laquelle la législation des États-Unis permet aux autorités publiques de collecter et de traiter des données transférées selon les principes de la sphère de sécurité. En particulier, les entreprises devraient être encouragées à indiquer, dans leurs politiques de protection de la vie privée, si elles dérogent auxdits principes pour répondre à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois.*

13. *Il importe que la dérogation pour raison de sécurité nationale prévue par la décision relative à la sphère de sécurité ne soit utilisée que dans la mesure où cela est strictement nécessaire et proportionné.*