COMMISSION EUROPEENNE

MÉMO

Bruxelles, le 27 novembre 2013

Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis — Foire aux questions

Que présente la Commission européenne aujourd'hui?

La Commission présente ce jour les actions qu'il conviendrait de mener pour rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis, en réponse aux vives préoccupations suscitées par les révélations sur les programmes américains de collecte de renseignements à grande échelle, qui ont mis à mal les relations transatlantiques.

La réponse que la Commission apporte aujourd'hui est développée dans plusieurs documents:

1. **un document de stratégie (en la forme d'une communication) sur les flux transatlantiques de données**, lequel expose les problèmes et les risques consécutifs aux révélations sur les programmes américains de collecte de renseignements, ainsi que les mesures qu'il conviendrait de prendre pour apaiser ces inquiétudes;
2. **une analyse du fonctionnement de la «sphère de sécurité»** qui régit les transferts de données à des fins commerciales entre l'Union européenne et les États-Unis;
3. **un rapport factuel sur les conclusions du groupe de travail ad hoc UE/États-Unis** sur la protection des données, créé au mois de juillet 2013;
4. un **examen** des accords en vigueur sur les **données des dossiers passagers (données PNR)** (voir MEMO/13/1054),
5. ainsi qu'un **réexamen** du **Programme de surveillance du financement du terrorisme (TFTP)** qui réglemente les échanges de données dans ces domaines à des fins répressives (voir MEMO/13/1164).

Pour maintenir des flux de données continus entre l'Union européenne et les États-Unis, il est impératif d'assurer un niveau élevé de protection des données. La Commission appelle aujourd'hui à agir dans six domaines:

1. adopter rapidement la **réforme de l'UE sur la protection des données**
2. rendre la **«sphère de sécurité»** plus sûre
3. renforcer les garanties en matière de protection des données dans le domaine **répressif**
4. recourir aux accords sectoriels et d'**entraide judiciaire** en vigueur pour obtenir des données

Spokespersons' Service
Service des Porte-parole

MEMO/13/1059

5. répondre aux préoccupations européennes dans le cadre de la **réforme en cours aux États-Unis**
6. promouvoir **des normes internationales de protection de la vie privée**.

1. La réforme de l'UE sur la protection des données: la réponse de l'Union aux craintes à l'égard des pratiques de surveillance

Comment la réforme de l'UE sur la protection des données répondra aux craintes à l'égard des pratiques de surveillance?

La réforme de l'UE sur la protection des données, proposée par la Commission au mois de janvier 2012 (IP/12/46), apporte des réponses essentielles en ce qui concerne la protection des données à caractère personnel. Cinq éléments du train de mesures proposé revêtent une importance particulière:

1. **Champ d'application territorial**: en réformant son régime de protection des données, l'Union veillera à ce que les entreprises non européennes respectent sa législation relative à la protection des données lorsqu'elles proposeront leurs produits et services aux consommateurs européens. Le droit fondamental à la protection des données sera ainsi respecté, quel que soit le lieu d'implantation géographique d'une société ou de son service de traitement de données.
2. **Transferts internationaux**: la proposition de règlement définit les conditions précises auxquelles seront subordonnés les transferts de données hors du territoire de l'Union. Ces transferts ne pourront être autorisés que si ces conditions, qui préservent les droits des personnes physiques à un niveau élevé de protection, sont réunies. Lors de son vote du 21 octobre, le Parlement européen a même proposé de durcir ces conditions.
3. **Contrôle de l'application:** les règles proposées prévoient des sanctions dissuasives pouvant aller jusqu'à 2 % du chiffre d'affaires annuel mondial de la société contrevenante (le Parlement européen a proposé de relever à 5 % le plafond des amendes) pour faire en sorte que les entreprises se conforment au droit de l'UE.
4. **Informatique en nuage**: la proposition de règlement énonce des dispositions claires sur les obligations et responsabilités qui incombent aux sous-traitants tels que les fournisseurs de services d'informatique en nuage, notamment en matière de sécurité. Comme l'ont montré les révélations sur les programmes américains de collecte de renseignements, il s'agit d'un point crucial car ces programmes s'intéressent aux données conservées dans le «nuage». En outre, les entreprises qui fournissent de l'espace de stockage dans le nuage et auxquelles des autorités étrangères demandent des données à caractère personnel ne pourront pas se soustraire à leur responsabilité en faisant valoir qu'elles ont le statut de sous-traitant et non de responsable du traitement des données.
5. **Services répressifs:** la réforme de la protection des données se traduira par l'édiction de règles très complètes visant à protéger les données à caractère personnel traitées dans le secteur répressif.

Prochaines étapes: les propositions de règlement et de directive relatifs à la protection des données sont actuellement examinées par le Parlement européen et le Conseil des ministres. Lors d'un vote, le 21 octobre 2013, le Parlement européen a résolument appuyé les propositions de la Commission, de sorte qu'il est prêt à entamer les négociations avec la seconde instance législative de l'Union, le Conseil de l'Union européenne. Lors d'un sommet, les 24 et 25 octobre 2013, les chefs d'État ou de gouvernement des États membres de l'Union ont, eux aussi, souligné l'importance d'adopter «en temps utile» la nouvelle législation sur la protection des données. La Commission souhaiterait que les négociations aboutissent d'ici au printemps 2014.

2. Rendre la «sphère de sécurité» plus sûre

Qu'est-ce que la décision relative à la sphère de sécurité?

La directive européenne de 1995 sur la protection des données régit le transfert de données à caractère personnel de l'UE vers des pays tiers. En vertu des dispositions de ce texte, la Commission peut décider qu'un pays tiers assure un «niveau de protection adéquat». Ces décisions sont généralement dénommées «décisions constatant le caractère adéquat du niveau de protection».

Sur la base de la directive susmentionnée, la Commission européenne a, le 26 juillet 2000, adopté une décision (la «décision relative à la sphère de sécurité») qui reconnaît que les «principes de la sphère de sécurité» et les «questions fréquemment posées», publiées par le ministère du commerce des États-Unis d'Amérique, assurent un niveau de protection adéquat pour les transferts de données à caractère personnel de l'UE.

En conséquence, la décision relative à la sphère de sécurité autorise le libre transfert de données à caractère personnel à des fins commerciales, entre des sociétés de l'UE et des entreprises établies aux États-Unis qui se sont engagées à respecter ces principes. Compte tenu des différences substantielles entre les régimes de protection de la vie privée en vigueur respectivement dans l'Union européenne et aux États-Unis, ces transferts seraient impossibles sans l'accord relatif à la sphère de sécurité.

Le fonctionnement du régime de la sphère de sécurité repose sur les engagements pris par les entreprises qui décident d'y souscrire et **l'autocertification** de celles-ci. Les sociétés qui s'engagent à respecter ces principes en informent le ministère du commerce des États-Unis; la commission fédérale du commerce contrôle, quant à elle, leur bonne mise en œuvre. **L'adhésion revêt un caractère volontaire, mais les règles sont contraignantes pour les entreprises qui y ont souscrit**. Les principes fondamentaux de cet accord sont les suivants:

- transparence des politiques de protection de la vie privée adoptées par les entreprises qui ont adhéré aux principes,
- intégration des principes de la sphère de sécurité dans les politiques de protection de la vie privée adoptées par les entreprises, et
- mise en œuvre («*enforcement*»), y compris par les autorités publiques.

Une entreprise américaine souhaitant adhérer aux principes de la sphère de sécurité doit: a) stipuler, dans la politique de protection de la vie privée qu'elle publie, son adhésion auxdits principes, et s'y conformer effectivement, et b) s'autocertifier, c'est-à-dire déclarer au ministère du commerce qu'elle est en conformité avec lesdits principes. L'autocertification doit être annuellement renouvelée.

Le contrôle de la mise en œuvre du régime de la sphère de sécurité aux États-Unis est confié au ministère du commerce et à la Commission fédérale du commerce de ce pays.

Combien de sociétés y recourent-elles?

À la fin du mois de septembre 2013, la sphère de sécurité comptait **3246 sociétés adhérentes** (soit huit fois plus de sociétés qu'en 2004, où elles n'étaient que 400).

Quel intérêt la sphère de sécurité présente-t-elle par rapport aux activités de surveillance?

Bien que la «sphère de sécurité» admette des limitations aux règles sur la protection des données, si des motifs liés à la sécurité nationale l'exigent, la question se pose de savoir si la collecte à grande échelle et le traitement d'informations à caractère personnel dans le cadre des programmes de surveillance américains sont nécessaires et proportionnés pour satisfaire aux intérêts de la sécurité nationale. La sphère de sécurité sert d'interface pour le transfert de données à caractère personnel de citoyens européens, de l'Union européenne vers les États-Unis, par les entreprises qui sont tenues de remettre des données aux agences américaines de renseignement dans le cadre de programmes américains de collecte de renseignements.

Comment se déroulerait, dans la pratique, un réexamen de la sphère de sécurité?

D'un point de vue juridique, la Commission européenne est compétente pour réexaminer la décision relative à la sphère de sécurité. La **Commission peut maintenir, suspendre ou adapter la décision** au vu des enseignements tirés de son application. Cela est notamment prévu en cas de défaillance systémique de la part des autorités américaines à faire respecter ces principes, 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 le niveau de protection garanti par les principes de la sphère de sécurité.

Que propose aujourd'hui la Commission européenne en ce qui concerne la «sphère de sécurité»?

Sur la base d'une analyse approfondie publiée ce jour et de consultations menées auprès de sociétés, la Commission européenne **formule 13 recommandations visant à améliorer le fonctionnement du régime de la sphère de sécurité**. Elle invite les autorités des États-Unis à dégager des solutions d'ici l'été 2014. La Commission révisera alors le fonctionnement du dispositif en se fondant sur la mise en œuvre de ces 13 recommandations.

Les 13 recommandations sont les suivantes:

Transparence

1. Les entreprises autocertifiées devraient rendre publiques leurs dispositions de protection de la vie privée.
2. Ces dispositions, publiées 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 des sociétés qui ont adhéré à la sphère de sécurité et dont la certification est «à jour».
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.

4. Sur son site web, le ministère du commerce devrait clairement signaler toutes les entreprises dont la certification n'est plus 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 chargé du règlement extrajudiciaire des litiges (REL).
6. Le REL devrait être facilement accessible et abordable économiquement.
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.

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. Chaque fois qu'un manquement est constaté, à la suite 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.

Accès des 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 au titre de la sphère de sécurité. En particulier, les entreprises devraient être encouragées à indiquer, dans leurs politiques de protection de la vie privée, quand 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 de ne recourir à la dérogation pour raison de sécurité nationale, prévue par la décision relative à la sphère de sécurité, que dans la mesure où cela est strictement nécessaire et proportionné.

Des informations relativement transparentes à cet égard sont fournies par certaines entreprises européennes adhérentes de la sphère de sécurité. **Nokia, par exemple**, qui est implantée aux États-Unis et souscrit à la sphère de sécurité, fournit l'information suivante dans 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.»*

Quels exemples illustrent-ils le mode de fonctionnement de la «sphère de sécurité»?

Le régime de la sphère de sécurité offre des solutions pour les transferts de données à caractère personnel dans les cas où d'autres outils n'existeraient pas ou ne fonctionneraient pas.

La société **Orange France** recourt aux services d'informatique en nuage proposés par Amazon U.S. aux fins de stockage de données. Pour que les données à caractère personnel concernant les clients d'Orange France puissent être transférées en dehors de l'UE, Amazon U.S. adhère aux principes de la sphère de sécurité, ce qui constitue une alternative à un accord contractuel particulier entre les deux sociétés qui s'appliquerait au traitement de données à caractère personnel transférées aux États-Unis.

Quant à une société d'envergure internationale comme **Mastercard**, qui est **établie aux États-Unis** mais possède de très nombreux clients dans l'UE, elle ne peut pas, pour transférer l'énorme volume de données à caractère personnel que requièrent ses opérations, recourir aux règles d'entreprise contraignantes car ces dernières ne s'appliquent qu'aux transferts effectués au sein d'un seul et même groupe de sociétés. Par ailleurs, des transferts réalisés en application de contrats seraient ingérables parce que Mastercard devrait alors en conclure des milliers, avec différentes institutions financières. Le régime de la sphère de sécurité offre, dès lors, la souplesse dont une telle structure internationale a besoin pour ses opérations, tout en permettant le libre transfert des données hors de l'UE, sous réserve du respect des principes de la sphère de sécurité

3. Renforcer les garanties en matière de protection des données dans le domaine répressif

Quel est l'objet de la négociation d'un accord-cadre sur la protection des données entre l'UE et les États-Unis à des fins répressives? Quel en est l'objectif?

L'Union européenne et les États-Unis négocient actuellement un accord-cadre sur la protection des données dans le domaine de la coopération policière et judiciaire (IP/10/1661). Dans ces négociations, l'Union entend obtenir un niveau élevé de protection des données, conformément à l'acquis de l'UE en la matière, pour les citoyens dont les données sont transférées de l'autre côté de l'Atlantique; la coopération entre l'UE et les États-Unis dans la lutte contre la criminalité et le terrorisme en sera renforcée.

La conclusion d'un tel accord, stipulant un niveau élevé de protection des données à caractère personnel, contribuerait grandement à accroître la confiance de part et d'autre de l'Atlantique. Au terme de la réunion ministérielle «Justice et affaires intérieures» entre l'UE et les États-Unis, le 18 novembre 2013, les deux parties se sont engagées à «achever les négociations relatives à cet accord avant l'été 2014».

Quelles sont les exigences de l'UE dans ces négociations?

Le niveau élevé de protection prévu pour les données à caractère personnel devrait se traduire par l'adoption de règles et de garanties portant sur un certain nombre de questions:

- accorder aux citoyens de l'Union qui ne sont pas résidents aux États-Unis des droits opposables, notamment le droit à un recours juridictionnel. À l'heure actuelle, la législation américaine ne permet pas aux Européens non résidents aux États-Unis de bénéficier des garanties conférées par le 1974 US Privacy Act (loi de 1974 sur la protection de la vie privée), qui réserve le recours juridictionnel aux ressortissants américains et aux résidents permanents légaux.

  Lors de la réunion ministérielle «Justice et affaires intérieures» entre l'UE et les États-Unis, l'engagement a été pris de traiter ce problème: «*Nous avons donc la volonté, parce qu'il y a urgence, de progresser rapidement dans les négociations en vue d'un accord-cadre constructif et global sur la protection des données dans le domaine répressif. Cet accord devrait servir de base pour faciliter les transferts de données dans le cadre de la coopération policière et judiciaire en matière pénale, en garantissant aux ressortissants américains et aux citoyens de l'UE un niveau élevé de protection des données à caractère personnel. Nous sommes déterminés à résoudre les dernières questions soulevées par les deux parties, y compris celle des voies de recours juridictionnel (question cruciale pour l'UE). Notre objectif est d'achever les négociations relatives à cet accord avant l'été 2014.*»;
- limitation des finalités: modalités et finalités du transfert et du traitement des données;
- conditions et durée de conservation des données;
- veiller à ce que la dérogation fondée sur la sécurité nationale reçoive une définition étroite.

Un accord-cadre allant dans ce sens devrait offrir le cadre général indispensable pour assurer un niveau élevé de protection des données à caractère personnel lorsque ces dernières sont transférées aux États-Unis aux fins de la prévention ou de la répression de la criminalité et du terrorisme. **L'accord ne constituerait toutefois pas la base juridique nécessaire pour procéder à des transferts particuliers de données à caractère personnel** entre l'UE et les États-Unis. Une base juridique propre, telle qu'une convention de transfert de données ou une loi nationale dans un État membre de l'UE, serait toujours requise à cet effet.

4. Utiliser l'accord d'entraide judiciaire en vigueur pour obtenir des données

Qu'est-ce que l'accord d'entraide judiciaire?

Les accords d'entraide judiciaire établissent une coopération entre différents pays en vue de réunir et d'échanger des informations, et de demander et de fournir une assistance pour obtenir des preuves situées dans un autre pays. Ils permettent aussi aux services répressifs de solliciter une entraide dans le cadre d'enquêtes ou de procédures pénales transfrontières. Des mécanismes ont été mis en place dans l'UE et aux États-Unis afin d'encadrer ces échanges.

L'accord entre l'UE et les États-Unis en matière d'entraide judiciaire est en vigueur depuis 2010. Il facilite et accélère l'aide en matière pénale entre l'UE et les États-Unis, notamment grâce à l'échange d'informations personnelles.

Si les autorités américaines contournent l'accord d'entraide judiciaire et accèdent directement aux données (par l'intermédiaire de sociétés) pour les besoins d'enquêtes pénales, elles exposent les sociétés opérant des deux côtés de l'Atlantique à d'importants risques juridiques. Ces sociétés pourraient, en effet, se retrouver en contravention avec la législation européenne ou américaine lorsqu'elles reçoivent de telles demandes: avec le droit américain (par exemple, le Patriot Act), si elles n'accordent pas l'accès aux données, et avec le droit européen, si elles l'accordent. Une solution consisterait dès lors, pour les autorités répressives américaines, à recourir aux voies officielles, telles que l'accord d'entraide judiciaire, lorsqu'elles demandent l'accès à des données à caractère personnel se trouvant dans l'UE et détenues par des sociétés privées.

Les négociations relatives à l'accord-cadre offrent l'occasion d'adopter des stipulations mentionnant noir sur blanc que les services répressifs ne pourront avoir accès, en dehors des canaux officiels de coopération tels que l'entraide judiciaire, aux données à caractère personnel détenues par des entités privées, sauf dans des cas bien déterminés, exceptionnels et soumis à un contrôle juridictionnel.

Qu'est-ce que le Patriot Act?

Le «U.S. Patriot Act» (loi patriotique) de 2001 est une loi votée par le Congrès américain et promulguée par le président George W. Bush le 26 octobre 2001. Il permet au Federal Bureau of Investigation (FBI) de demander une ordonnance judiciaire enjoignant à une entreprise ou une autre entité de produire des «choses corporelles» telles que des registres, des dossiers ou des documents, lorsque les informations recherchées sont utiles à une enquête pour obtenir des renseignements étrangers ne concernant pas un ressortissant américain ou pour protéger le pays contre le terrorisme international ou des activités de renseignement clandestines. L'ordonnance du tribunal est secrète et ne peut pas être divulguée.

Au cours des réunions du groupe de travail ad hoc UE-États-Unis, ces derniers ont confirmé que cette loi pouvait servir de base juridique à la collecte de renseignements, lesquels peuvent comprendre, selon le programme, des métadonnées téléphoniques (par exemple, les numéros de téléphone composés, ainsi que la date, l'heure et la durée des appels) ou le contenu des communications.

5. Répondre aux préoccupations européennes dans le contexte de la réforme en cours aux États-Unis

Comment la révision des programmes de surveillance américains bénéficiera-t-elle aux citoyens de l'UE?

Le président américain Barack Obama a annoncé un réexamen des activités des autorités américaines chargées de la sécurité nationale, y compris du cadre juridique applicable. Ce processus constitue une occasion importante de répondre aux préoccupations de l'Union européenne suscitées par les récentes révélations sur les programmes américains de collecte de renseignements. Les modifications les plus importantes consisteraient dans l'**application aux citoyens de l'UE ne résidant pas aux États-Unis des mêmes garanties que celles dont bénéficient les ressortissants et résidents américains**, la **transparence accrue** des activités de renseignement et le **renforcement des contrôles**.

Une plus grande transparence est, en effet, requise en ce qui concerne, d'une part, le cadre juridique des programmes américains de collecte de renseignements et son interprétation par les tribunaux américains et, d'autre part, la dimension quantitative desdits programmes. Les citoyens de l'UE bénéficieraient également de ces modifications.

Le contrôle des programmes américains de collecte de renseignements pourrait être amélioré par le renforcement du rôle de la Foreign Intelligence Surveillance Court américaine et par l'instauration de voies de recours pour les particuliers. Ces mécanismes pourraient réduire le traitement des données à caractère personnel concernant des Européens qui ne sont pas pertinentes pour la protection de la sécurité nationale.

Ces modifications rétabliraient la confiance dans les échanges de données entre l'UE et les États-Unis et dans l'économie numérique.

Qu'en est-il de la législation fédérale américaine sur la protection de la vie privée?

En mars 2013, immédiatement après l'adoption des propositions de réforme de la Commission, la Maison Blanche a annoncé qu'elle travaillerait de concert avec le Congrès pour faire voter une «déclaration des droits à la vie privée des consommateurs» (Consumer Privacy Bill of Rights).

Les récents débats au Congrès témoignent du fait qu'aux États-Unis aussi, on attache une importance croissante à la protection de la vie privée. Selon un sondage IPSOS publié en janvier 2013, 45 % des Américains adultes estiment avoir peu ou pas de maîtrise du tout sur leurs données à caractère personnel sur internet. De plus, il n'existe pas de loi fédérale unique protégeant les données, mais une multitude de lois votées par les États fédérés, offrant des degrés variables de sécurité. En Floride, il n'existe pas une seule loi définissant la notion de «personal information» (informations personnelles), alors qu'en Arizona, il y en a cinq. Il en va de même pour les règles concernant les atteintes à la sécurité: certains États fédérés en ont, d'autres pas.

Dès lors que l'Union aura adopté un corps unique et cohérent de règles de protection des données, nous attendrons des États-Unis qu'ils fassent de même. C'est indispensable pour créer une base stable pour les échanges de données à caractère personnel entre les deux côtés de l'Atlantique. L'interopérabilité et un système d'autorégulation ne sauraient suffire. Un corps de règles strictes et opposables en matière de protection des données, inscrites à la fois dans le droit de l'UE et dans la législation américaine, constituerait une base solide pour les flux transfrontières de données.

6. Promouvoir des normes internationales de protection de la vie privée

Que peut-on faire au niveau mondial?

Les questions que soulèvent les méthodes modernes de protection des données ne se limitent pas aux transferts de données entre l'Union européenne et les États-Unis. Toute personne devrait également se voir garantir un niveau élevé de protection des données la concernant. Il conviendrait, dès lors, de promouvoir à l'échelle internationale les règles de l'UE en matière de collecte, de traitement et de transfert de données.

De même qu'ils ont adhéré à la convention de 2001 sur la cybercriminalité, les États-Unis devraient adhérer à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («convention 108»).

Les normes de protection des données feront-elles partie des négociations en cours en vue d'un partenariat transatlantique de commerce et d'investissement?

Non. Les normes de protection des données ne feront pas partie des points abordés dans le cadre de ces négociations. La Commission européenne l'annonce très clairement dans la communication publiée aujourd'hui.

Cette exclusion a été confirmée par la vice-présidente Viviane Reding et le commissaire Karel De Gucht à plusieurs reprises. Ainsi que M^{me} Reding le mentionnait récemment dans un discours: «*La protection des données, ce n'est ni de la bureaucratie ni un tarif douanier. C'est un droit fondamental et, à ce titre, elle n'est pas négociable*.» (SPEECH/13/867)

7. Groupe de travail ad hoc UE-États-Unis sur la protection des données

Quand le groupe de travail ad hoc UE-États-Unis sur la protection des données a-t-il été créé?

Ce groupe ad hoc a été créé en juillet 2013 pour se pencher sur les questions soulevées par les révélations concernant plusieurs programmes de surveillance américains reposant sur la collecte à grande échelle et le traitement d'informations à caractère personnel. L'objectif était d'établir les faits entourant ces programmes de surveillance et leurs conséquences sur les données à caractère personnel des citoyens de l'Union.

Le Conseil de l'Union européenne a également décidé de mettre en place une «deuxième voie», dans le cadre de laquelle les États membres peuvent aborder avec les autorités américaines, de façon bilatérale, des questions touchant à la sécurité nationale et des aspects liés à la surveillance supposée des institutions et des missions diplomatiques de l'Union européenne.

Combien de réunions ont-elles eu lieu à ce jour?

Il y a eu quatre réunions. Une réunion préparatoire a eu lieu à Washington, le 8 juillet 2013. Le groupe s'est ensuite réuni les 22 et 23 juillet 2013 à Bruxelles, les 19 et 20 septembre 2013 à Washington, et le 6 novembre 2013 à Bruxelles.

Qui participe au groupe de travail?

Du côté de l'UE, le groupe de travail ad hoc est coprésidé par la Commission et la présidence du Conseil de l'Union européenne. Il est composé de représentants de la présidence en exercice, des services de la Commission (DG Justice et DG Affaires intérieures), du Service européen pour l'action extérieure, de la prochaine présidence, du coordinateur de l'UE de la lutte contre le terrorisme, du président du groupe de travail «article 29» (au sein duquel se réunissent les autorités nationales chargées de la protection des données), ainsi que de dix experts originaires des États membres sélectionnés dans le domaine de la protection des données et de la répression/sécurité. Du côté américain, le groupe est composé de hauts fonctionnaires du ministère de la justice, du Bureau du directeur du renseignement national, du ministère des affaires étrangères et du ministère de la sécurité intérieure.

Quelles ont été les principales conclusions du groupe de travail?

Les principales conclusions du groupe de travail ont été les suivantes:

- Un certain nombre de lois américaines **autorisent la collecte à grande échelle et le traitement des données à caractère personnel** qui ont été transmises aux États-Unis ou sont traitées par des entreprises américaines, **à des fins de renseignement étranger**. Les États-Unis ont confirmé l'existence et les principaux éléments de certains aspects de ces programmes, dans le cadre desquels la collecte et le traitement de données ont lieu en vertu de dispositions légales américaines qui fixent des conditions spécifiques et des garanties.
- Il existe des différences entre les garanties applicables aux citoyens de l'UE et celles dont bénéficient les ressortissants américains dont les données sont traitées. Le niveau des garanties prévues pour les premiers est inférieur, de même que le seuil fixé pour la collecte de données à caractère personnel les concernant. En outre, alors que des procédures concernant le ciblage et la réduction au minimum de la collecte de données existent pour les ressortissants américains, elles ne s'appliquent pas aux citoyens de l'UE, même lorsqu'ils n'ont aucun lien avec le terrorisme, la criminalité ou toute autre activité illicite ou dangereuse. Les ressortissants américains bénéficient de protections constitutionnelles (respectivement, premier et quatrième amendements), mais celles-ci ne s'appliquent pas non plus aux citoyens de l'UE qui ne résident pas sur le territoire des États-Unis.
- Un manque de clarté subsiste quant à l'utilisation de certaines bases juridiques existantes qui autorisent la collecte des données (comme certains «Executive Order 12333»), à l'existence d'autres programmes de surveillance, ainsi qu'aux limitations applicables à ces derniers.
- Puisque les ordonnances de la Foreign Intelligence Surveillance Court sont secrètes et que les sociétés sont tenues de garder le secret sur l'assistance qu'elles sont obligées de fournir, il n'y a aucune possibilité (judiciaire ou administrative) pour les personnes concernées, européennes ou américaines, de savoir si des données à caractère personnel les concernant font l'objet d'une collecte ou d'un traitement ultérieur. **Les particuliers n'ont pas la possibilité d'obtenir l'accès aux données les concernant, ni de les faire rectifier ou effacer, et ils n'ont pas non plus de recours administratif ou judiciaire.**
- Bien qu'un certain degré de contrôle soit exercé par les trois branches du gouvernement dans des cas spécifiques, notamment un contrôle juridictionnel pour les activités impliquant une faculté de contraindre à fournir des informations, **le pouvoir judiciaire ne se prononce pas sur la façon dont les données collectées sont demandées**: il n'est pas demandé aux juges d'approuver les «sélectionneurs» et les critères employés pour examiner les données et extraire des éléments d'information utilisables. Il n'y a pas non plus de contrôle juridictionnel de la collecte de renseignements étrangers à l'extérieur des États-Unis, laquelle est réalisée dans le cadre de la seule compétence du pouvoir exécutif.

Pour de plus amples informations:

Communiqué de presse sur les transferts de données entre l'UE et les États-Unis:

IP/13/1166