COMMISSION
EUROPÉENNE

Bruxelles, le 29.4.2016
COM(2016) 238 final

2016/0127 (NLE)

Proposition de

DÉCISION DU CONSEIL

concernant la signature, au nom de l'Union européenne, d'un accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

• Justification et objectifs de la proposition

Un groupe de contact à haut niveau (ci-après le «HLCG»), composé de hauts fonctionnaires de la Commission, de représentants de la présidence du Conseil et des ministères de la justice, de la sécurité intérieure et des affaires étrangères des États-Unis, a été mis sur pied en novembre 2006 en vue d'étudier les moyens qui permettraient à l'UE et aux États-Unis de coopérer plus étroitement et plus efficacement dans le domaine de l'échange d'informations en matière répressive, tout en veillant à garantir la protection des données à caractère personnel et de la vie privée. La conclusion présentée en octobre 2009 par le HLCG dans son rapport final[1] était qu'un accord international engageant tant l'UE que les États-Unis à appliquer des principes communs reconnus en matière de protection des données pour les transferts de données transatlantiques dans le domaine répressif constituait la meilleure option: un tel accord aurait l'avantage d'établir les fondements d'une protection efficace de la vie privée et des données à caractère personnel régissant tout échange d'informations en matière répressive, et il offrirait le niveau de sécurité juridique le plus élevé.

Le 3 décembre 2010, le Conseil a adopté une décision autorisant la Commission à ouvrir des négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique relatif à la protection des données à caractère personnel lors de leur transfert et de leur traitement à des fins de prévention et de détection des infractions pénales, dont le terrorisme, d'enquêtes et de poursuites en la matière, dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale (ci-après l'«accord-cadre»)[2].

La Commission a engagé les négociations le 28 mars 2011. Le 8 septembre 2015, les Parties ont paraphé le texte.

L'accord-cadre établit (pour la première fois) un cadre complet de principes et de garanties en matière de protection des données lors du transfert d'informations à caractère personnel[3] à des fins d'application du droit pénal entre les États-Unis, d'une part, et l'Union européenne ou ses États membres, d'autre part. Son double objectif est de garantir un niveau élevé de protection des données et, partant, d'améliorer la coopération entre les Parties. Bien qu'il ne constitue pas en soi la base juridique de transferts d'informations à caractère personnel vers les États-Unis, l'accord-cadre complète, en tant que de besoin, les garanties en matière de protection

---

1 Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection [Rapports du groupe de contact à haut niveau (HLCG) sur le partage d'informations et la protection de la vie privée et la protection des données à caractère personnel], Bruxelles, 23 novembre 2009, 15851/09, JAI 822 DATAPROTECT 74 USA 102.

2 Parallèlement à l'adoption de la réforme de la réglementation européenne en matière de protection des données et du nouveau «bouclier de protection des données UE-États-Unis» concernant les transferts de données dans le domaine commercial, la conclusion d'un accord-cadre pertinent et exhaustif constitue un élément capital de la stratégie exposée dans la communication de la Commission intitulée «Rétablir la confiance dans les flux de données entre **l'Union** européenne et les États-Unis», COM(2013) 846 final du 27 novembre 2013, disponible à l'adresse http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52013DC0846&qid=1460547233920&from=FR. Cela a d'ailleurs été réaffirmé dans les orientations politiques du président Juncker et dans la communication de la Commission au Parlement européen et au Conseil intitulée «Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides», COM(2016) 117 final du 29 février 2016, disponible à l'adresse http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52016DC0117&rid=1

3 La notion d'«informations à caractère personnel» utilisée dans l'accord-cadre est synonyme de celle de «données à caractère personnel» figurant dans le droit de l'UE.

des données figurant dans les accords existants et futurs relatifs au transfert de données ou les dispositions nationales autorisant ce type de transfert.

Il s'agit d'une amélioration substantielle par rapport à la situation actuelle, dans laquelle des informations à caractère personnel sont transférées de l'autre côté de l'Atlantique sur la base d'instruments juridiques (accords internationaux ou législations nationales) dont les dispositions en matière de protection des données sont généralement limitées, voire inexistantes.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

L'accord-cadre renforcera la protection reconnue pour toutes les données à caractère personnel des personnes concernées de l'Union lors de leur échange avec les États-Unis à des fins d'application du droit pénal. En établissant un cadre complet de garanties en matière de protection des données, l'accord complétera les accords existants (aussi bien les accords bilatéraux entre les États membres et les États-Unis que les accords UE-États-Unis) sur la base desquels des données à caractère personnel sont transférées aux États-Unis à des fins répressives lorsque, et dans la mesure où, lesdits accords n'offrent pas le niveau exigé de protection et de garanties.

L'accord fournira en outre un «filet de sécurité» pour les futurs accords UE/États membres-États-Unis, correspondant au niveau minimal de protection exigé. Il s'agit là d'une garantie importante pour l'avenir et d'une évolution majeure par rapport à la situation actuelle, où garanties, protections et droits doivent être négociés à nouveau pour chaque nouvel accord.

Dans l'ensemble, l'accord-cadre apportera une valeur ajoutée importante par l'augmentation du niveau de protection dont jouiront les personnes concernées de l'Union, dans le respect des exigences du droit primaire et dérivé de l'Union. Il mettra en place pour la première fois un instrument de protection des données couvrant de manière exhaustive et cohérente tous les transferts de données dans un domaine déterminé (c'est-à-dire les échanges transatlantiques de données dans le domaine de la coopération policière et judiciaire en matière pénale). L'accord-cadre soutiendra en outre, dans le contexte transatlantique, les exigences générales relatives aux transferts internationaux de données figurant dans la future directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données (ci-après la directive «police»)[4], adoptée le 14 avril 2016. Compte tenu de ce qui précède, l'accord-cadre crée aussi un précédent important pour d'éventuels accords comparables à passer avec d'autres partenaires internationaux.

- **Cohérence avec les autres politiques de l'Union**

L'accord-cadre devrait avoir des effets considérables en matière de coopération policière et répressive avec les États-Unis. En établissant un cadre commun et exhaustif de règles et garanties en matière de protection des données, il permettra à l'UE ou à ses États membres, d'une part, et aux services répressifs pénaux des États-Unis, d'autre part, d'instaurer entre eux

[4] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012) 10 final – 2012/0010 (COD), disponible à l'adresse http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012PC0010&from=fr

une coopération plus efficace. En outre, il fera en sorte que les accords existants contiennent toutes les garanties nécessaires en termes de protection. Cette mesure assurera la continuité de la coopération en matière répressive, tout en renforçant la sécurité juridique en cas de transfert de données. Par ailleurs, l'accord-cadre facilitera la conclusion de futurs accords de transfert de données avec les États-Unis dans le domaine répressif, étant donné que les garanties relatives à la protection des données auront fait l'objet d'un accord et ne devront donc plus être renégociées à chaque fois. Enfin, l'instauration de normes communes dans ce domaine de coopération essentiel mais complexe est une réalisation importante susceptible de contribuer sensiblement à rétablir la confiance dans les flux transatlantiques de données.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La base juridique de la présente proposition est l'article 16 du TFUE, en liaison avec l'article 218, paragraphe 5, du TFUE.

• Subsidiarité

L'accord-cadre relève de la compétence exclusive de l'Union européenne, en vertu de l'article 3, paragraphe 2, du TFUE. Par conséquent, le principe de subsidiarité ne s'applique pas.

• Proportionnalité

L'accord-cadre prévoit les garanties en matière de protection des données requises en vertu des directives de négociation du Conseil. Elles sont considérées comme des éléments nécessaires pour garantir le niveau de protection requis, à la fois par la Charte des droits fondamentaux et compte tenu de l'évolution de l'acquis de l'UE, lorsque des données à caractère personnel sont transférées vers un pays tiers. Ni une liste nettement plus restreinte de garanties en la matière, ni un instrument d'une force obligatoire moindre ne peuvent être considérés comme suffisants pour assurer un tel niveau de protection. Par conséquent, la proposition ne va pas au-delà de ce qui est nécessaire pour atteindre l'objectif politique consistant à établir un cadre pour la protection des données à caractère personnel lors de leur transfert entre les États-Unis, d'une part, et l'Union européenne ou ses États membres, d'autre part, dans un contexte répressif.

• Choix de l'instrument

La mise en place d'un cadre contraignant pour la protection des données à caractère personnel, qui complétera les accords existants et constituera la base d'accords futurs, ne peut être assurée que par un accord international conclu entre l'Union européenne et les États-Unis.

En outre, comme cela a été souligné dans le rapport du HLCG d'octobre 2009, un accord international garantit le niveau de sécurité juridique le plus élevé.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

• Évaluations ex post/bilans de qualité de la législation existante

Sans objet.

- **Consultation des parties intéressées**

La Commission a régulièrement rendu compte, tant oralement que par écrit, de l'avancement des négociations au comité spécial du Conseil désigné. Le Parlement européen a été tenu régulièrement informé, par l'intermédiaire de sa commission des libertés civiles, de la justice et des affaires intérieures (LIBE), à la fois oralement et par écrit.

- **Obtention et utilisation d'expertise**

L'initiative met en œuvre les directives de négociation adoptées par le Conseil le 3 décembre 2010.

- **Analyse d'impact**

Aucune analyse d'impact n'a été nécessaire. L'accord proposé est conforme aux directives de négociation du Conseil.

- **Réglementation affûtée et simplification**

Sans objet.

- **Droits fondamentaux**

Les dispositions de l'accord-cadre visent à protéger le droit fondamental à la protection des données à caractère personnel ainsi que le droit à un recours effectif et à un procès équitable, consacrés respectivement par les articles 8 et 47 de la Charte des droits fondamentaux de l'Union européenne.

4. INCIDENCE BUDGÉTAIRE

L'accord proposé n'a pas d'incidence budgétaire.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Une mise en œuvre de la part des États membres sera nécessaire mais aucune modification majeure des législations n'est à attendre, étant donné que les dispositions de fond de l'accord-cadre correspondent dans une large mesure à des règles déjà applicables aux autorités européennes et nationales en vertu du droit de l'Union et/ou du droit national.

Explication détaillée des différentes dispositions de la proposition

L'accord-cadre contient cinq catégories de dispositions, comme le prévoyaient les directives de négociation du Conseil: i) dispositions horizontales; ii) principes et garanties en matière de protection de données; iii) droits individuels; iv) aspects relatifs à l'application de l'accord et au contrôle; v) dispositions finales.

i) Dispositions horizontales

i) Objet de l'accord (article 1)

Pour atteindre l'objectif de l'accord, à savoir assurer un niveau élevé de protection des informations à caractère personnel et renforcer la coopération dans le domaine répressif, l'accord-cadre établit un cadre pour la protection des informations à caractère personnel lors de leur transfert entre les États-Unis, d'une part, et l'UE ou ses États membres, d'autre part, à

des fins de prévention et de détection des infractions pénales, dont le terrorisme, d'enquêtes et de poursuites en la matière. La référence aux notions de «prévention, détection, enquêtes et poursuites en matière d'infractions pénales» (ci-après désignées collectivement par les expressions «application du droit (pénal)» ou «domaine répressif/matière répressive») garantit que le présent accord sera compatible avec l'architecture de l'acquis de l'UE actuel et futur en matière de protection des données [notamment la distinction, quant à leur couverture respective, entre le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données («règlement général sur la protection des données»[5]) et la directive «police»].

En indiquant que l'accord-cadre ne saurait, en soi, constituer la base juridique d'éventuels transferts d'informations à caractère personnel et qu'une base juridique (distincte) est toujours requise, l'article 1 précise également que l'accord-cadre est un accord portant véritablement sur les droits fondamentaux et établissant un ensemble de protections et de garanties applicables à ces transferts.

ii) Définitions (article 2)

Les termes clés de l'accord-cadre sont définis à l'article 2. Les définitions des notions «informations à caractère personnel», «traitement des informations à caractère personnel», «Parties», «État membre» et «autorité compétente» correspondent, sur le fond, à celles données à ces concepts dans d'autres accords UE-États-Unis et/ou dans l'acquis de l'UE en matière de protection des données.

iii) Champ d'application de l'accord (article 3)

L'article 3 de l'accord-cadre en définit le champ d'application. Il garantira que les protections et garanties prévues par l'accord-cadre s'appliquent à tous les échanges de données ayant lieu dans le cadre de la coopération transatlantique des services répressifs en matière pénale. Il s'agit des transferts s'effectuant sur la base de lois nationales, d'accords UE-États-Unis (tels que le traité d'entraide judiciaire entre l'UE et les États-Unis), d'accords entre les États membres et les États-Unis (tels que les traités d'entraide judiciaire, les accords sur le renforcement de la coopération en matière de prévention et de répression des formes graves de criminalité, les accords ou arrangements sur les données de détection du terrorisme), ainsi que sur la base d'accords spécifiques prévoyant le transfert de données à caractère personnel par des entités privées à des fins répressives [par exemple au titre de l'accord UE-États-Unis sur les dossiers passagers[6] («PNR») et de l'accord sur le programme de surveillance du financement du terrorisme[7] (accord «TFTP»)]. Le champ d'application est défini sur la base du transfert de données, c'est-à-dire qu'il couvre en principe tous les transferts de données à des fins d'application du droit pénal entre l'UE et les États-Unis, indépendamment de la nationalité ou du lieu de résidence de la personne concernée.

---

5 Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012) 11 final — 2012/0011 (COD), disponible à l'adresse: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52012PC0011&qid=1460734213424&from=FR

6 Accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers (données PNR) et leur transfert au ministère américain de la sécurité intérieure, JO L 215 du 11.8.2012, p. 5.

7 Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO L 195 du 27.7.2010, p. 5.

L'accord-cadre ne couvrira pas les transferts de données à caractère personnel (ou d'autres formes de coopération) entre les autorités des États-Unis et les autorités des États membres chargées d'assurer la sécurité nationale.

iv) Non-discrimination (article 4)

L'article 4 prévoit que chaque Partie met en œuvre l'accord-cadre sans discrimination arbitraire ou injustifiée entre ses propres ressortissants et ceux de l'autre Partie.

Cet article complète et renforce d'autres dispositions de l'accord (notamment les articles offrant des garanties aux personnes en matière d'accès, de rectification et de recours administratif – voir ci-dessous). Il garantit en effet que les citoyens européens bénéficieront en principe d'une égalité de traitement avec les citoyens des États-Unis dans le cadre de l'application pratique de ces dispositions par les autorités des États-Unis.

v) Effet de l'accord (article 5)

En ce qui concerne les accords déjà conclus entre l'Union/les États membres et les États-Unis, l'accord-cadre les complétera en tant que de besoin, c'est-à-dire si, et dans la mesure où, ils n'offrent pas les garanties indispensables en matière de protection des données[8].

La mise en œuvre effective de l'accord-cadre (et notamment de ses articles relatifs aux droits individuels) entraîne une présomption de compatibilité avec les règles applicables en matière de transfert international de données. Cette présomption n'est ni automatique ni générale et, comme toutes les présomptions, elle peut être renversée. Il ne s'agit pas d'une présomption automatique parce que son application dépend expressément de la mise en œuvre effective de l'accord-cadre par les États-Unis et, plus particulièrement – ainsi que l'explicite l'article 5, paragraphe 2 – de la mise en œuvre effective des articles portant sur les droits des personnes (notamment en matière d'accès, de rectification, de recours administratif et juridictionnel). Il ne s'agit pas non plus d'une présomption générale: étant donné que l'accord-cadre ne constitue pas un instrument «autonome» pour la réalisation de transferts, une telle présomption s'applique nécessairement au cas par cas, c'est-à-dire en évaluant si la combinaison de l'accord-cadre et de la base juridique spécifique du transfert offre un niveau de protection conforme aux règles de protection des données de l'UE. Autrement dit, contrairement à une décision constatant le caractère adéquat du niveau de protection, cette clause ne prévoit pas la reconnaissance «en bloc» du niveau de protection offert aux États-Unis en tant que tel, ni une autorisation générale des transferts.

ii) Principes et garanties en matière de protection des données

Les articles décrits ci-après couvrent d'importants principes régissant le traitement des données à caractère personnel, ainsi que des garanties et restrictions essentielles.

i) Limitation des finalités et de l'utilisation (article 6)

Dans le respect de la Charte des droits fondamentaux de l'UE et de l'acquis de l'UE, l'article 6 applique le principe de la limitation des finalités à tous les transferts de données à

[8] Le quatrième considérant du préambule précise que l'accord-cadre ne modifie pas et ne subordonne pas à certaines conditions les accords établissant qu'ils offrent un niveau suffisant de protection des données, et qu'il ne déroge pas à de tels accords. Fait exception la disposition relative au recours juridictionnel figurant à l'article 19, qui s'applique aussi à ces accords. Cela concerne les accords PNR et TFTP.

caractère personnel couverts par l'accord-cadre, tant dans le cas de transferts liés à des affaires spécifiques que lors de la conclusion, entre les États-Unis et l'UE ou ses États membres, d'un accord autorisant des transferts en masse de données à caractère personnel. Le traitement (qui inclut le transfert) peut uniquement avoir lieu pour des finalités explicites et légitimes relevant du champ d'application de l'accord-cadre, à savoir à des fins de prévention et de détection des infractions pénales, dont le terrorisme, d'enquêtes et de poursuites en la matière.

En outre, le traitement ultérieur d'informations à caractère personnel par d'autres autorités (services répressifs, autorités réglementaires ou administratives) que la première autorité destinataire d'une Partie est autorisé à condition qu'il ne soit pas incompatible avec les finalités pour lesquelles les données ont été initialement transférées, et que lesdites autres autorités respectent toutes les autres dispositions de l'accord-cadre.

L'autorité compétente émettrice peut aussi imposer des conditions supplémentaires (par exemple sur l'utilisation des données) dans des affaires spécifiques.

Enfin, le traitement d'informations à caractère personnel ne peut intervenir que s'il est directement pertinent et n'est pas excessif ou trop général au regard de ses finalités.

L'article 6 est une disposition clé de l'accord: il assure l'application des garanties au «cycle de vie» complet d'un ensemble de données considéré, depuis son transfert initial au départ de l'UE jusqu'à son traitement par une autorité compétente des États-Unis et vice-versa, y compris son éventuel transfert ultérieur à une autre autorité des États-Unis ou son traitement par une telle autorité, ou, dans le cas d'un transfert de données au départ des États-Unis vers une autorité compétente de l'Union ou de (l'un de) ses États membres, son transfert ultérieur éventuel à une autre autorité de l'UE ou d'un État membre ou son traitement par une telle autorité.

ii) Transfert ultérieur (article 7)

Les restrictions relatives au transfert ultérieur énoncées à l'article 7 impliquent que si une autorité américaine a l'intention de transférer à son tour des données qu'elle a reçues de l'UE ou de l'un de ses États membres à un pays tiers/une organisation internationale non liés par l'accord, elle doit au préalable obtenir l'autorisation de l'autorité répressive de l'UE ayant transféré initialement les données vers les États-Unis. Cette règle s'applique également dans le cas où une autorité de l'UE ou de l'un de ses États membres a l'intention de transférer des données qu'elle a reçues des États-Unis à un pays tiers/une organisation internationale.

Lorsqu'elle statue sur une demande d'autorisation, l'autorité émettrice initiale devra tenir dûment compte de tous les facteurs pertinents, notamment la finalité pour laquelle les données ont été transférées initialement, et le fait que le pays tiers ou l'organisation internationale destinataire offre un niveau approprié de protection des informations à caractère personnel. Elle peut aussi subordonner le transfert à certaines conditions.

Par ailleurs, à l'instar des articles relatifs à la limitation des finalités (voir article 6 ci-dessus), à la durée de conservation des données (voir article 12 ci-dessous) et aux données sensibles (voir article 13 ci-dessous), l'article 7 prend expressément en compte le caractère particulièrement sensible du transfert en masse des données de personnes non soupçonnées (par exemple les données PNR de tous les passagers prenant un vol, indépendamment de tout soupçon concret à leur égard), en ce qu'il dispose que tout transfert ultérieur d'informations à caractère personnel autres que des informations se rapportant à des affaires précises est

subordonné au respect de certaines conditions définies dans l'accord justifiant dûment ledit transfert.

La situation spécifique des transferts ultérieurs vers un autre État membre à l'intérieur de l'UE (par exemple, le partage, par la police française, d'informations reçues du FBI américain avec la police allemande) est également traitée dans cet article (au paragraphe 4). Il est prévu que si, en vertu des règles applicables, de tels transferts sont subordonnés à une autorisation préalable, l'autorité qui a transmis initialement les informations (par ex. le FBI américain) ne pourra refuser son autorisation ou imposer des conditions en invoquant la protection des données (étant donné que toutes les autorités concernées sont liées par l'accord-cadre).

iii) Préservation de la qualité et de l'intégrité des informations (article 8)

Les Parties prendront des mesures raisonnables pour que les données à caractère personnel transférées soient conservées avec l'exactitude, la pertinence, l'actualité et l'exhaustivité nécessaires et appropriées à un traitement licite des informations. Lorsque l'autorité destinataire ou émettrice a connaissance de doutes sérieux quant à la pertinence, l'actualité, l'exhaustivité ou l'exactitude de données à caractère personnel reçues ou transférées, elle doit en aviser dans la mesure du possible l'autorité émettrice/destinataire.

iv) Sécurité des informations (article 9) et notification d'un incident relatif à la sécurité des informations (article 10)

Ces articles contribuent à assurer un niveau élevé de sécurité des données à caractère personnel échangées par les Parties à l'accord-cadre.

Premièrement, en vertu de l'article 9, les Parties mettront en place des dispositifs techniques, organisationnels et de sécurité appropriés pour protéger les informations à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle et la divulgation, la modification, l'accès ou tout autre traitement non autorisé. Ces dispositifs prévoiront aussi que seul le personnel habilité se verra accorder l'accès aux données à caractère personnel.

Deuxièmement, en vertu de l'article 10, en cas d'incident de sécurité présentant un risque important de préjudice, des mesures appropriées doivent être prises rapidement pour atténuer le préjudice, notamment la notification de l'incident à l'autorité émettrice et, le cas échéant en fonction des circonstances de l'incident, à la personne concernée. Les exceptions à l'obligation de notification sont énumérées de manière exhaustive dans la disposition en question et correspondent à des limitations raisonnables (par exemple la sécurité nationale).

v) Tenue de dossiers (article 11)

Les Parties mettent en place des méthodes efficaces (tels que des journaux) pour démontrer la licéité du traitement et de l'utilisation des informations à caractère personnel.

Cette exigence constitue une garantie appréciable pour les personnes car elle impose aux autorités répressives la charge de démontrer qu'une opération de traitement de données a été effectuée en conformité avec la loi. L'obligation de documenter les opérations de traitement de données implique, en particulier, qu'un traitement illicite laissera une «trace», ce qui devrait faciliter le traitement des plaintes et l'introduction de réclamations concernant la licéité des traitements.

vi) Durée de conservation (article 12)

Le traitement de données sera subordonné à la fixation de durées de conservation précises, pour garantir que les données ne seront pas conservées plus longtemps que ce qui est nécessaire et approprié. Différents éléments devront être pris en considération pour fixer ces durées de conservation, notamment la finalité du traitement ou de l'utilisation, la nature des données et l'incidence sur les droits et intérêts des personnes touchées.

Il est également indiqué que, lorsque les Parties concluent un accord sur le transfert de «données en masse», ledit accord doit contenir une disposition spécifique sur la durée de conservation applicable. Grâce à cette disposition, les Parties acceptent le principe selon lequel de tels accords de transfert en masse doivent être assortis d'une durée de conservation spécifique, principe qui ne devra donc pas être négocié à nouveau.

Les durées de conservation seront réexaminées périodiquement, afin de déterminer si des circonstances nouvelles imposent une modification de la durée de conservation applicable.

Dans un souci de transparence, les durées de conservation devront être publiées ou portées à la connaissance du grand public par d'autres moyens.

vii) Catégories particulières de données (article 13)

Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou autres, l'appartenance à un syndicat, ou le traitement d'informations à caractère personnel relatives à la santé ou à la vie sexuelle, ne peut avoir lieu que lorsque des garanties appropriées sont établies conformément à la législation (par exemple en masquant les informations une fois atteinte la finalité pour laquelle le traitement a eu lieu ou en exigeant que l'accès à ces informations soit subordonné à l'autorisation d'une autorité de contrôle).

Les accords permettant le «transfert en masse» de données à caractère personnel devront préciser les normes et conditions selon lesquelles des catégories particulières de données pourront être traitées.

Les dispositions relatives aux catégories particulières de données sont compatibles avec l'exigence selon laquelle le traitement doit être directement pertinent et non excessif, en vertu de l'article 6 sur la limitation des finalités et de l'utilisation.

viii) Prise de décision automatisée (article 15)

Un traitement de données susceptible d'aboutir à des décisions ayant des effets négatifs pour une personne (par exemple dans le cadre du profilage) ne peut pas être fondé exclusivement sur le traitement automatisé d'informations à caractère personnel, sauf si le droit interne l'autorise, et à condition qu'il existe des garanties appropriées, notamment la possibilité d'obtenir une intervention humaine.

ix) Transparence (article 20)

Les personnes sont habilitées à recevoir des informations (au moyen de notifications générales ou individuelles, et sous réserve de «restrictions raisonnables») sur la finalité du traitement et l'éventuelle utilisation ultérieure qui peut être faite des données à caractère personnel les concernant, les dispositions législatives ou réglementaires régissant ce traitement, l'identité des tiers auxquels leurs informations à caractère personnel peuvent être divulguées, ainsi que les mécanismes d'accès, de rectification et de recours disponibles.

Le fait de mieux informer les personnes sur les raisons pour lesquelles les données les concernant sont traitées, et sur l'identité des organismes qui effectuent ces traitements, contribue à leur permettre d'exercer leurs droits d'accès, de rectification ou de recours (voir articles 16-19 ci-dessous).

iii) Droits individuels

Ces droits revêtent une importance particulière pour la protection des personnes concernées. Celles-ci seront en mesure, pour la première fois, de se prévaloir de droits de portée générale au regard de tout transfert transatlantique de données à caractère personnel dans le domaine répressif.

i) Accès et rectification (articles 16 et 17)

Le droit d'accès permet à toute personne de demander et d'obtenir l'accès aux données à caractère personnel la concernant. Les motifs d'une restriction d'accès sont énoncés de manière exhaustive et correspondent à des restrictions raisonnables (par exemple garantir la sécurité nationale, éviter de nuire à une enquête ou aux poursuites relatives à des infractions pénales, protéger les droits et libertés d'autres personnes). L'accès à ses propres données ne peut être subordonné à des dépenses excessives.

Le droit de rectification permet à toute personne de demander la correction ou la rectification des données à caractère personnel la concernant si ces dernières sont inexactes ou ont été traitées de manière abusive. La rectification peut notamment consister à compléter, effacer ou verrouiller des données, ou en d'autres mesures ou méthodes destinées à remédier aux inexactitudes ou au traitement abusif.

Lorsque l'autorité compétente du pays destinataire conclut, à la suite d'une demande présentée par une personne, d'une notification émanant du fournisseur des informations à caractère personnel, ou à la suite de sa propre enquête, que les informations sont inexactes ou ont fait l'objet d'un traitement abusif, elle prend des mesures pour les compléter, les effacer, les verrouiller, ou d'autres mesures de correction ou de rectification.

Lorsque le droit national l'autorise, toute personne est en droit de mandater une autorité de contrôle (c'est-à-dire, pour une personne concernée de l'UE, une autorité nationale chargée de la protection des données) pour demander en son nom l'accès ou la rectification. Cette possibilité d'exercer leurs droits de manière indirecte par l'intermédiaire d'une autorité et dans le cadre d'un système juridique qui leur est familier devrait, concrètement, aider les personnes concernées lorsqu'elles cherchent à faire respecter leurs droits.

Si une demande d'accès ou de rectification est refusée ou restreinte, l'autorité saisie doit fournir à la personne (ou à son représentant dûment mandaté) une réponse exposant les raisons de ce refus ou de cette restriction. L'obligation de fournir à l'intéressé une réponse motivée vise à permettre et faciliter l'exercice de son droit de recours administratif et juridictionnel en cas de refus ou de restriction de l'accès/la rectification de la part de l'autorité répressive concernée.

ii) Recours administratif (article 18)

Si une personne n'accepte pas le résultat de sa demande d'accès/de rectification portant sur des données à caractère personnel la concernant, elle a le droit d'introduire un recours administratif. À l'instar de ce qui est prévu en matière d'accès et de rectification, la personne

concernée peut, pour faciliter l'exercice effectif de ce droit, mandater une autorité de contrôle (c'est-à-dire une autorité nationale chargée de la protection des données, dans le cas d'une personne concernée de l'UE) ou un autre représentant, lorsque le droit interne applicable le permet.

L'autorité à laquelle il est demandé réparation adressera à la personne concernée une réponse écrite indiquant, le cas échéant, les améliorations ou corrections apportées.

iii) Recours juridictionnel (article 19)

Les citoyens de chaque Partie doivent avoir la possibilité de former un recours juridictionnel contre i) le refus d'accès, ii) le refus de rectification ou iii) la divulgation illicite par les autorités de l'autre Partie.

Du côté américain, ce droit est concrétisé par le «Judicial Redress Act», signé par le président Obama le 24 février 2016. Cet acte étendra aux citoyens des «pays couverts»[9] ces trois motifs de recours juridictionnel prévus par le «Privacy Act» américain de 1974, mais dont ne pouvaient se prévaloir jusqu'ici que les citoyens ou résidents permanents des États-Unis. Le quatrième considérant du préambule de l'accord-cadre précise que cette extension couvrira aussi les données échangées au titre d'accords tels que les accords PNR et TFTP. En combinaison avec l'adoption du «Judicial Redress Act», l'article 19 améliorera donc sensiblement la protection judiciaire dont bénéficient les citoyens de l'UE.

Bien que le «Judicial Redress Act» comporte certaines restrictions (en particulier, il s'appliquera uniquement aux données des citoyens des «pays couverts» dont les données ont été transférées par des autorités répressives de l'UE, c'est-à-dire notamment, mais pas uniquement, les citoyens de l'UE), l'article 19 de l'accord-cadre répond à une exigence de longue date de l'UE.

Cette disposition correspond aux orientations politiques du président Juncker, selon lesquelles «*Les États-Unis doivent […] garantir que tous les citoyens de l'UE, qu'ils résident ou non aux États-Unis, ont le droit de faire valoir leurs droits à la protection des données devant les tribunaux américains. Ce point sera essentiel pour rétablir la confiance dans les relations transatlantiques.*» Elle fait également suite à la résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA américaine, dans laquelle le Parlement a demandé «*une reprise immédiate des négociations avec les États-Unis sur l'accord-cadre, en vue de placer les droits des citoyens de l'Union européenne sur un pied d'égalité avec ceux des ressortissants des États-Unis […]*» et qu'il soit permis «*à tous les citoyens de l'Union d'introduire des recours […] judiciaires efficaces et exécutoires aux États-Unis sans aucune discrimination*»[10].

---

9 Un «pays couvert», dans le cadre du «Judicial Redress Act» américain, est un pays: i) qui a conclu avec les États-Unis un accord prévoyant des mesures de protection appropriées de la vie privée en ce qui concerne les informations échangées à des fins répressives (ou qui a effectivement échangé des informations à des fins répressives et s'est doté de mesures de protection appropriées de la vie privée en ce qui concerne de tels échanges d'informations); ii) qui autorise le transfert de données à caractère personnel à des fins commerciales, par un accord avec les États-Unis ou un autre mécanisme; iii) dont les politiques concernant le transfert de données à caractère personnel à des fins commerciales ne nuisent pas gravement aux intérêts de la sécurité nationale des États-Unis. C'est le ministre de la justice des États-Unis (Attorney General) qui déclare un pays «pays couvert».

10 Voir le point 57 et le considérant BJ de la résolution du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits

Le paragraphe 3 de l'article 19 précise que l'extension des trois motifs de recours juridictionnel susmentionnés est sans préjudice des autres voies de recours juridictionnel disponibles à d'autres titres en ce qui concerne le traitement des données (par exemple au titre de l'Administrative Procedure Act, de l'Electronics Communication Privacy Act ou du Freedom of Information Act). Ces autres bases juridiques d'un recours juridictionnel sont ouvertes à toutes les personnes concernées de l'UE dont les données sont transférées à des fins répressives, indépendamment de leur nationalité ou de leur lieu de résidence.

iv) Aspects liés à l'application de l'accord-cadre et contrôle

i) Obligation de rendre compte (article 14)

Des mesures doivent être mises en place afin de promouvoir l'obligation de rendre compte des autorités qui traitent des données à caractère personnel couvertes par l'accord-cadre. En particulier, lorsque l'autorité destinataire transfère des données à caractère personnel à d'autres autorités, ces dernières devraient être averties des garanties qui s'appliquent au titre de l'accord-cadre, ainsi que des éventuelles conditions (restrictives) supplémentaires dont le transfert est assorti en application de l'article 6, paragraphe 3 (sur la limitation des finalités et de l'utilisation). Les fautes graves doivent être l'objet de sanctions pénales, civiles ou administratives appropriées et dissuasives.

Les mesures visant à promouvoir l'obligation de rendre compte comprennent également, le cas échéant, l'arrêt des transferts ultérieurs de données à caractère personnel à des entités des Parties non couvertes par l'accord-cadre si elles n'assurent pas une protection efficace des informations à caractère personnel, compte tenu de l'objet de l'accord (et notamment des dispositions relatives à la limitation des finalités et aux transferts ultérieurs). Cette disposition concerne la situation où des données à caractère personnel sont transmises par une autorité de l'UE à une autorité fédérale des États-Unis (autrement dit, une autorité couverte par l'accord-cadre) puis transférées à une autorité répressive au niveau d'un État fédéré. Les règles constitutionnelles des États-Unis limitent la capacité de l'État fédéral à engager les États fédérés au niveau international[11]. Cependant, pour assurer la continuité de la protection des données transférées à des agences fédérales des États-Unis puis partagées avec des agences répressives au niveau des États fédérés, l'article 14: i) inclut, dans son champ d'application, les «autres autorités» des Parties (c'est-à-dire les autorités non couvertes par l'accord, telles que celles des États fédérés des États-Unis); ii) précise que les garanties prévues au titre de l'accord-cadre doivent leur être notifiées; et iii) prévoit que, le cas échéant, les transferts à ces autorités doivent être interrompus si celles-ci ne protègent pas efficacement les données à caractère personnel, compte tenu de l'objet de l'accord-cadre et notamment de ses articles relatifs à la limitation des finalités et aux transferts ultérieurs.

En visant à faire en sorte que les autorités répressives compétentes soient tenues pour responsables du respect de l'accord-cadre, cet article est un élément important pour l'efficacité du système d'application et de contrôle mis en place au titre de l'accord. Il

---

fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures [2013/2188(INI)], disponible à l'adresse suivante: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//FR

[11] Les États-Unis étant une république fédérale, il existe un partage des compétences entre le gouvernement fédéral et les gouvernements des États fédérés (voir aussi, à cet égard, l'article 5, paragraphe 2, de l'accord-cadre).

facilitera également l'introduction de réclamations en cas de faute (et, partant, de responsabilité d'autorités publiques).
Enfin, les autorités de l'UE seront à même de soulever des préoccupations auprès de leurs homologues américaines, et d'en recevoir des informations pertinentes, sur la manière dont elles s'acquittent de leurs obligations au titre de l'article 14 (y compris sur les mesures prises à cet égard). Par ailleurs, dans le cadre des réexamens conjoints (voir article 23 ci-dessous), une attention particulière sera accordée à la mise en œuvre effective de cet article.

ii) Contrôle effectif (article 21)

Les Parties mettent en place une ou plusieurs autorités publiques qui exercent en toute indépendance des fonctions et des pouvoirs de contrôle, y compris de réexamen, d'enquête et d'intervention. Ces autorités sont compétentes pour connaître des plaintes des particuliers à l'égard des mesures d'application de l'accord-cadre et y faire droit, ainsi que pour signaler les infractions à la législation liée au présent accord aux fins d'une action pénale ou disciplinaire. Compte tenu des particularités du système américain, un ensemble d'autorités de contrôle [directeurs généraux chargés de la protection de la vie privée (*Chief Privacy Officers*), inspecteurs généraux (*Inspector Generals*), commission de surveillance du respect de la vie privée et des libertés civiles (*Privacy and Civil Liberties Oversight Board*), etc.] exerceront de manière cumulative les fonctions de contrôle assumées dans l'UE par les autorités chargées de la protection des données.

Cet article complète les garanties qu'offrent les dispositions en matière d'accès, de rectification et de recours administratif. Il permet notamment aux personnes de déposer plainte auprès d'autorités indépendantes sur la manière dont l'autre Partie a mis en œuvre l'accord-cadre.

iii) Coopération entre les autorités de contrôle (article 22)

Les autorités de contrôle coopéreront en vue d'assurer la mise en œuvre effective de l'accord, notamment en ce qui concerne le système d'exercice indirect des droits individuels en matière d'accès, de rectification et de recours administratif (voir articles 16 à 18 ci-dessus).

En outre, des points de contact nationaux sont établis pour aider à déterminer l'autorité de contrôle à laquelle s'adresser dans une affaire donnée. Compte tenu notamment de l'existence de différentes autorités de contrôle aux États-Unis, la création d'un «point d'entrée» central pour les demandes d'assistance et de coopération vise à faciliter un traitement efficace de ces demandes.

iv) Réexamen conjoint (article 23)

Les Parties procéderont à des réexamens périodiques conjoints de la mise en œuvre et de l'efficacité de l'accord-cadre, en accordant une importance particulière à la mise en œuvre effective des articles relatifs aux droits individuels (accès, rectification, recours administratif et juridictionnel) ainsi qu'à la question des transferts aux entités territoriales non couvertes par l'accord (c.-à-d. les États fédérés des États-Unis). Le premier réexamen conjoint sera réalisé au plus tard trois ans après l'entrée en vigueur de l'accord et, ensuite, à intervalles réguliers.

Les délégations des Parties comprendront des représentants des autorités chargées de la protection des données et des autorités répressives/judiciaires; les conclusions des réexamens conjoints seront rendues publiques.

v) Dispositions finales

L'accord-cadre contient une série de clauses finales concernant:

- la notification à l'autre Partie de tout instrument législatif ou réglementaire affectant substantiellement la mise en œuvre de l'accord. Les États-Unis informeront notamment l'UE de toute mesure relative à l'application des dispositions du Judicial Redress Act (article 24);
- les consultations à mener si un litige survient à propos de l'interprétation ou de l'application de l'accord (article 25);
- la possibilité, pour une Partie, de suspendre l'accord en cas de violation substantielle de l'accord par l'autre Partie (article 26);
- l'application territoriale de l'accord, afin de tenir compte de la situation particulière du Royaume-Uni, de l'Irlande et du Danemark (article 27);
- la durée illimitée de l'accord (justifiée d'une part par la nature de l'accord, qui est un cadre offrant protection et garanties, et d'autre part par la possibilité de suspendre et de dénoncer l'accord (article 28);
- la possibilité pour chacune des Parties de dénoncer l'accord par notification à l'autre Partie, bien qu'il soit précisé que les informations à caractère personnel transférées avant la dénonciation continueront d'être traitées conformément aux règles de l'accord-cadre (article 29, paragraphes 2 et 3);
- l'entrée en vigueur de l'accord, le premier jour du mois suivant la date à laquelle les Parties ont échangé les notifications indiquant qu'elles ont parachevé leurs procédures d'approbation internes (article 29, paragraphe 1);
- la clause linguistique (qui précède immédiatement la ligne de signature), prévoyant: i) la signature de l'accord en anglais et l'établissement par l'UE de ses versions dans les 23 autres langues officielles de l'Union; ii) la possibilité, après la signature, d'authentifier la version de l'accord dans chacune de ces autres langues officielles de l'UE par échange de notes diplomatiques avec les États-Unis; iii) en cas de divergence entre différentes versions linguistiques faisant foi de l'accord, la primauté de la version anglaise.

2016/0127 (NLE)

Proposition de

DÉCISION DU CONSEIL

concernant la signature, au nom de l'Union européenne, d'un accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16 en liaison avec l'article 218, paragraphe 5,

vu la proposition de la Commission européenne,

considérant ce qui suit:

(1) Le 3 décembre 2010, le Conseil a autorisé la Commission à ouvrir des négociations avec le gouvernement des États-Unis d'Amérique en vue d'un accord relatif à la protection des données à caractère personnel lors de leur transfert et de leur traitement à des fins de prévention et de détection des infractions pénales, dont le terrorisme, d'enquêtes et de poursuites en la matière.

(2) Les négociations avec le gouvernement des États-Unis d'Amérique ont été menées à bien et le texte de l'accord a été paraphé le 8 septembre 2015.

(3) L'accord vise à établir un cadre complet de principes et de garanties en matière de protection des données lors du transfert d'informations à caractère personnel à des fins d'application du droit pénal entre les États-Unis, d'une part, et l'Union européenne ou ses États membres, d'autre part. Son objectif est de garantir un niveau élevé de protection des données et, partant, d'améliorer la coopération entre les Parties. Bien qu'il ne constitue pas en soi la base juridique de transferts d'informations à caractère personnel vers les États-Unis, l'accord-cadre complète, en tant que de besoin, les garanties en matière de protection des données figurant dans les accords existants et futurs relatifs au transfert de données ou les dispositions nationales autorisant ce type de transfert.

(4) Les compétences de l'Union couvrent toutes les dispositions de l'accord. L'Union a notamment adopté la directive 2016/XXX/UE[12] relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

[12] Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

(5) L'Union européenne dispose d'une compétence exclusive dans la mesure où l'accord est susceptible d'affecter des règles communes de l'Union ou d'en altérer la portée.

(6) Conformément à l'article 6 *bis* du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE, le Royaume-Uni et l'Irlande ne sont pas liés par les règles fixées dans l'accord portant sur le traitement de données à caractère personnel dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 (Coopération judiciaire en matière pénale) ou du chapitre 5 (Coopération policière) du titre V de la troisième partie du TFUE, lorsque le Royaume-Uni et l'Irlande ne sont pas liés par les règles qui imposent le respect de l'accord.

(7) Conformément aux articles 1er et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente décision et n'est donc pas lié par l'accord ni soumis à son application.

(8) Il convient de signer l'accord, sous réserve de sa conclusion à une date ultérieure,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La signature, au nom de l'Union européenne, de l'accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière est autorisée, sous réserve de la conclusion dudit accord.

Le texte de l'accord qui doit être signé est joint à la présente décision.

Article 2

Le Secrétariat général du Conseil élabore l'instrument de pleins pouvoirs autorisant la personne indiquée par la Commission à signer l'accord, sous réserve de sa conclusion.

Article 3

La présente décision entre en vigueur le jour de son adoption.

Fait à Bruxelles, le

Par le Conseil
Le président