Observations du CEPD concernant divers accords internationaux, notamment les accords PNR UE-US et UE-AUS, l'accord TFTP UE-US, ainsi que la nécessité d'une approche globale des accords internationaux relatifs à l'échange de données

I. Les accords PNR

Le CEPD a formulé plusieurs observations concernant **l'accord PNR entre l'UE et les États-Unis**, en particulier dans ses interventions devant la Cour de justice[1] et dans ses avis[2] adoptés conjointement avec le groupe de travail «Article 29».

Plusieurs de ces observations n'ont pas été prises en compte dans la version définitive de l'accord et restent donc valables. Depuis, l'accord est entré en vigueur à titre provisoire, bien qu'il n'ait pas été conclu de manière officielle, et des possibilités d'évaluation de son efficacité sont apparues à plusieurs reprises. Le niveau de protection offert par l'accord doit, dès lors, être évalué également à la lumière des aspects pratiques de sa mise en œuvre. Les points ci-dessous résument nos conclusions antérieures en tenant compte de cette perspective.

Outre la question de la base juridique de l'accord, l'analyse a principalement porté sur le niveau de protection adéquat offert par l'accord, conformément à l'article 25 de la directive 95/46/CE[3] et à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

- *Limitation de la finalité:* Le champ d'application de l'accord ne se limite pas uniquement à la lutte contre le terrorisme. Parmi les finalités citées, figurent les intérêts vitaux de tout individu ou une obligation légale. Un champ d'application aussi large pose des questions de sécurité juridique et exerce également une influence sur l'appréciation du juste équilibre entre le caractère intrusif et le caractère nécessaire de ces mesures.

- *Qualité et proportionnalité des données:* la liste des données à caractère personnel pouvant être collectées est très détaillée et comporte même des données sensibles dans des cas exceptionnels, ainsi que des données concernant des tierces personnes, c'est-à-dire des données ne concernant pas

[1] Affaires C-317/04 et C-318/04.

[2] Consultez les différents avis du groupe de travail «Article 29» sur les données PNR des États-Unis en cliquant sur le lien suivant : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/index_en.htm#data_transfers

[3] L'évaluation du caractère adéquat de la protection se base sur une liste de critères publiée dans un document de travail (WP12) du groupe «Article 29». Ce document de travail «Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données», adopté le 24 juillet 1998, peut-être consulté en cliquant sur le lien suivant : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_fr.pdf.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

uniquement les passagers du vol aérien. La durée de stockage de ces données (15 ans) est jugée excessive;

- *Légitimité du traitement des données:* la collecte de données ne concerne pas uniquement les individus représentant un risque: l'accord prévoit une collecte en masse des données personnelles et une évaluation des risques identique pour tous les individus, ce qui entraîne nécessairement le traitement de données à caractère personnel d'une grande majorité de personnes innocentes. La collecte, l'analyse et le stockage à une si grande échelle de données à caractère personnel pourraient donner lieu à des problèmes de légitimité et de proportionnalité au vu de la jurisprudence de la Cour européenne des droits de l'homme (voir, en particulier, l'affaire S. et Marper [4]);

- *Sécurité juridique:* le caractère obligatoire des engagements du CBP n'est pas clair étant donné que des éléments décisifs de l'accord sont inclus dans une lettre annexe. Cela pourrait amener les États-Unis à interpréter leurs obligations de manière unilatérale;

- *Transferts ultérieurs:* l'accord prévoit de nombreuses possibilités de transferts ultérieurs, en incluant des exceptions floues aux principes de protection des données: notamment des "situations d'urgence" qui autorisent de tels transferts;

- *Droits individuels:* bien que des voies de recours soient prévues dans l'accord, en pratique, l'exercice des droits par les individus, en particulier le droit d'accès aux données à caractère personnel, reste problématique: des exceptions liées à des raisons de sécurité pourraient empêcher l'exercice concret de ces droits.

- *Système «Push/pull»:* le passage d'un système «pull» (système d'extraction) à un système «push» (système d'exportation), afin que les compagnies aériennes contrôlent les données transmises aux États-Unis, est loin d'avoir atteint un niveau acceptable en pratique. L'enquête menée par le sous-groupe "passagers" du groupe de travail «Article 29» confirme cette lacune importante[5].

- *Efficacité de la mise en œuvre et du réexamen:* le niveau adéquat ne sera atteint que s'il existe des garanties de l'application des principes et de la sanction des violations de manière efficace, proportionnée et dissuasive. Les conditions de réexamen posent certaines questions d'ordre pratique: dans l'accord, les autorités chargées de la protection des données ne sont pas mentionnées comme prenant part au réexamen. Elles sont susceptibles d'être effectivement impliquées, mais il n'existe aucune sécurité juridique quant à leur rôle et leur autonomie en ce qui concerne les conditions pratiques et les conclusions du réexamen.

Pour conclure sur ce point, l'accord UE-US doit faire l'objet d'une évaluation qui tienne compte non seulement des lacunes identifiées au moment de la négociation de l'accord mais également du contexte global de sa mise en œuvre. L'organisation éventuelle d'un réexamen

[4] S. et Marper c Royaume-Uni, du 4 décembre 2008, requêtes n^{os} 30562/04 et 30566/04.

[5] Se référer également à la réponse du président du groupe de travail «Article 29» à votre lettre, relative aux accords PNR.

dans les semaines ou mois à venir permettrait indéniablement d'apporter des éléments utiles pour compléter l'estimation actuelle.

L'accord UE-AUS est moins problématique que l'accord UE-US et la majorité des remarques soulevées lors des négociations de l'accord a été prise en considération. Néanmoins, des améliorations pourraient être apportées sur les points suivants:

- la durée de stockage des données, plus courte que dans l'accord avec les États-Unis (5 ans et demi), est encore jugée trop longue;
- le nombre de données transférées, dont les données sensibles;
- les conditions de réexamen de l'accord.

S'agissant de la mise en œuvre effective de l'accord, les principaux enjeux aujourd'hui concernent la mise en place d'un système «Push» efficace ainsi que le nombre de données requises par les douanes australiennes.

Le sous-groupe «Données passagers» du groupe de travail «Article 29», dans lequel le CEPD est impliqué, suit de très près les progrès de la mise en œuvre des accords PNR avec l'Australie et les États-Unis. À cet égard, des informations complémentaires sont fournies par le président du groupe de travail «Article 29» en réponse à votre lettre.

II. L'accord TFTP UE-US

Le CEPD a suivi attentivement l'évolution de la situation concernant les transferts de données financières du système SWIFT aux autorités américaines et a publié, en juillet dernier, des observations relatives au mandat de négociation proposé par la Commission en vue d'un accord entre l'UE-US. Récemment, le CEPD a activement contribué à la lettre conjointe rédigée par le groupe de travail «Article 29» et le groupe «Police et Justice».

Vu l'ensemble de ces informations, les observations ci-dessous, en sus des observations formulées par le groupe de travail «Article 29» et le groupe «Police et Justice», apporteront un complément d'informations concernant principalement les questions soulevées dans votre lettre.

Principe de nécessité, proportionnalité et sécurité juridique. Les mesures envisagées dans l'accord TFTP portent fortement atteinte à la vie privée, car elles interfèrent avec la vie privée de tous les citoyens européens, compte tenu également du recours de plus en plus fréquent aux transferts bancaires (transfrontaliers) au sein de la zone européenne. Conformément à l'article 8 de la CEDH et au cadre législatif de l'UE, une telle interférence doit être établie par la loi et prévisible, ainsi que nécessaire pour atteindre l'intérêt commun recherché.

Dans cette perspective, il doit exister des preuves très solides de la nécessité et de la proportionnalité de telles mesures intrusives. Cela implique qu'il faut également démontrer que ces dites mesures présentent une valeur ajoutée concrète, notamment en comparaison d'autres instruments de l'UE portant moins atteinte à la vie privée qui visent à combattre l'exploitation du système financier à des fins de blanchiment de capitaux et de financement du terrorisme (par exemple, la directive 2005/60/CE relative à la prévention du blanchiment de capitaux et le règlement (CE) n°1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds).

Les preuves fournies jusqu'à présent au CEPD ne démontrent pas totalement la nécessité et la réelle valeur ajoutée par rapport à d'autres instruments déjà existants et plus ciblés,

notamment les instruments spécifiques pour l'échange d'informations entre Europol, Eurojust et les États-Unis, ainsi que l'accord UE-US en matière d'entraide judiciaire. Contrairement à l'accord PNR, l'accord TFTP ne prévoit aucun lien entre les données traitées et les États-Unis: le contrôleur est établi en Europe, les bases de données se trouvent en Europe et les données transférées aux États-Unis concernent tous les types de transactions financières dans le monde (telles que, dans la plupart des cas, des virements au sein de la communauté européenne et des virements d'Europe vers des pays tiers).

Concernant la sécurité juridique et la prévisibilité, de nombreux éléments importants relatifs à la protection des données sont toujours absents ou mal définis dans l'accord (voir les observations ci-dessous).

Limitation de la finalité et qualité des données (notamment l'aspect de la conservation des données). Conformément aux remarques exprimées par le CEPD à plusieurs reprises, le traitement de données commerciales à des fins répressives constitue une dérogation au principe de limitation de la finalité et doit, par conséquent, être limité et ciblé. Dans cette perspective, le CEPD insiste sur le rôle primordial d'un contrôle judiciaire indépendant de l'évaluation de la légalité des injonctions des États-Unis demandant des données et reconnaît que le processus de demandes établi à l'article 4 de l'accord va dans la bonne direction.

Toutefois les transferts en masse prévus par l'article 4, paragraphe 6, de l'accord comme des cas exceptionnels constituent une source d'inquiétude, le recours à ces transferts n'étant pas clairement limité et pouvant fort bien devenir une pratique courante.

La définition de la finalité pour laquelle les données peuvent être transférées est plus large que celle énoncée à l'article 1 de la décision-cadre du Conseil (2002/475/JAI) relative à la lutte contre le terrorisme.

Il n'est pas prouvé que la durée de stockage de données non-extraites (5 ans) doive être considérée comme proportionnée. En outre, l'accord ne précise pas la durée de stockage des données extraites. Il ne prévoit pas non plus de dispositifs garantissant que les données extraites et non-extraites seront effacées dès qu'elles ne sont plus nécessaires à une enquête visant à lutter contre le terrorisme.

De plus, le partage des données à caractère personnel avec d'autres autorités nationales ou pays tiers n'est pas clairement défini ni ne bénéficie de garanties appropriées, comme l'exigeraient les dispositions de la Convention 108 et de la Décision-cadre 2008/977/JAI.

Droits des personnes affectées par ces mesures, responsabilité et révision judiciaire. L'accord traite uniquement des droits des personnes concernées dans son article 11, paragraphe 1, qui fait référence au droit d'obtenir la confirmation de l'autorité chargée de la protection des données "*que toutes les vérifications nécessaires ont bien été menées au sein de l'Union européenne pour s'assurer que ses droits en matière de protection des données ont été respectés conformément au présent accord*". En outre l'article 11, paragraphe 3, stipule qu'un droit de recours administratif et juridictionnel effectif pour d'éventuelles violations du présent accord est prévu en application de la législation de l'Union européenne, de ses États membres et des États-Unis.

Ces dispositions soulèvent diverses questions. Premièrement, l'article 11, paragraphe 1, limite les vérifications de respect des droits de protection des données à la seule Union européenne et ne prévoit pas ces mêmes garanties pour les États-Unis où se déroulera pourtant la partie la plus sensible du traitement des données européennes. Deuxièmement, la même disposition

prévoit d'éventuelles restrictions quant à la possibilité qu'ont les autorités chargées de la protection des données de mener ces vérifications, avec une clause sans précédent et dont la logique est difficile à appréhender. Troisièmement - ce qui est plus essentiel encore - de nombreux droits des personnes concernées, comme, par exemple, la rectification, l'information, la compensation pour traitement illicite, les voies de recours, n'ont pas été pris en compte ou la manière de les respecter ne fait pas l'objet d'une définition claire et concrète, si ce n'est la référence très générale que fait l'article 11, paragraphe 3, au droit interne des parties contractantes respectives.

À cet égard, le CEPD insiste sur le fait que l'article 8 de la Charte des droits fondamentaux de l'Union européenne stipule clairement que "*toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification*" et que "*le respect de ces règles est soumis au contrôle d'une autorité indépendante*".

Dans ce contexte, le réexamen conjoint prévu par l'article 10 ne peut être considéré comme substitut de la surveillance indépendante requise par le cadre juridique de l'Union européenne.

En outre, l'article 10, paragraphe 2, n'impose des limites quant au nombre de représentants participant à ce réexamen que pour les autorités de protection des données.

L'article 16 TFUE comme base juridique et l'approche pour un éventuel accord futur. Le CEPD déplore que, dans la dernière version de la décision de Conseil relative à la conclusion de l'accord provisoire (5305/1/10 REV 1 du 21 janvier 2010), la référence à l'article 16 TFUE comme une des bases juridiques pertinentes a été supprimée.

À cet égard, le CEPD est fermement convaincu que, puisque cet accord concerne essentiellement l'échange de données à caractère personnel, l'article 16 constitue une base juridique tout aussi pertinente que les autres dispositions du TFUE relatives à la coopération des services répressifs. L'importance de l'article 16 du TFUE, également soulignée lors de l'audition de M^{me} Reding devant votre Commission, est évidente si l'on veut éviter que l'accord international ne repose uniquement sur l'aspect répressif.

Dans la même logique, le CEPD est satisfait que l'accord actuel ne soit conclu que pour une durée limitée et qu'il stipule clairement qu'il ne constitue pas un précédent. Un nouvel accord sera entièrement négocié selon ce nouveau cadre juridique et fera nécessairement l'objet d'une nouvelle analyse qui reprendra de façon exhaustive l'ensemble des éléments requis par les normes de l'UE en matière de protection des libertés fondamentales et qui profitera pleinement du nouveau rôle du Parlement européen dans ce domaine précis. Le nouvel accord devra traiter attentivement certaines questions qui ne l'ont pas été parfaitement en raison de l'urgence de conclure un accord provisoire.

Conclusion. En conclusion, s'agissant de l'accord TFTP, le CEPD considère que trop peu d'éléments ont encore été fournis jusqu'à présent pour justifier la nécessité et la proportionnalité d'un accord si invasif dans la sphère de la vie privée, qui, à bien des égards, empiète sur d'autres instruments européens et internationaux déjà existants dans ce domaine.

En outre, certains points de cet accord ne sont pas définis de façon suffisamment claire pour être prévisibles pour les Européens dont les données sont transférées aux États-Unis. Certes, l'accord règle certaines questions soulevées par les autorités européennes chargées de la protection des données (telles que le mécanisme de contrôle judiciaire indépendant établi par le présent article 4), mais il ne prévoit pas de façon satisfaisante et systématique toutes les garanties requises par le cadre juridique de l'UE relatif à la protection des données, ce qui

laisse des lacunes dangereuses qui devraient faire l'objet d'un examen attentif, à la lumière de l'article 16 du TFUE et du nouveau cadre juridique établi par le traité de Lisbonne.

III. Le besoin d'une approche globale des accords internationaux relatifs à l'échange de données

Le CEPD souhaiterait souligner que ces différents accords conclus avec des pays tiers, notamment les États-Unis, ne prévoient pas de cadre harmonisé et cohérent en matière d'échange d'informations transfrontaliers.

Dans ce contexte, le projet actuellement négocié d'un accord transatlantique en matière d'application de la loi avec les États-Unis mérite une attention particulière. Il reste à apprécier de quelle manière ce nouvel instrument horizontal pourrait s'appliquer aux accords déjà existants. Toutefois, un tel cadre harmonisé pourrait très probablement renforcer la sécurité juridique.

Le CEPD est en faveur d'une telle initiative, à condition que le niveau de protection offert par l'accord soit suffisamment élevé et que des mesures d'exécution fortes soient prévues.

Bruxelles, le 25 janvier 2010