Avis du Contrôleur européen de la protection des données sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP II)

(2010/C 355/02)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1],

vu la demande d'avis formulée conformément à l'article 28, paragraphe 2, du règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [2],

A ADOPTÉ L'AVIS SUIVANT

I. INTRODUCTION

1. Le 15 juin 2010, la Commission a adopté une proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (TFTP) (ci-après «la proposition»). La proposition (comprenant le texte d'un projet d'accord avec les États-Unis) a été envoyée au CEPD pour consultation. Le CEPD se félicite d'avoir été consulté et recommande que le présent avis soit mentionné dans les considérants de la proposition.

2. La proposition de la Commission a été motivée par des changements dans l'architecture de SWIFT [3] qui, à partir du 1er janvier 2010, garantit que les messages de transactions financières de SWIFT qui sont internes à l'Espace économique européen et à la Suisse resteront dans la zone européenne — et non dans la zone transatlantique — et ne seront plus copiés au centre d'exploitation américain.

3. Dans la proposition actuelle, la Commission envisage la conclusion d'un accord international entre l'Union européenne et les États-Unis, fondé sur les articles 216 (accords internationaux), 82 (coopération judiciaire) et 87 (coopération policière) du traité sur le fonctionnement de l'Union européenne, qui exigerait le transfert au département du Trésor des États-Unis de données de messagerie financière pertinentes, nécessaires aux fins du programme de surveillance du financement du terrorisme du département du Trésor des États-Unis.

4. Suite à la décision du Parlement européen du 11 février 2010 de s'opposer à l'accord intérimaire signé le 30 novembre 2009, le nouveau projet vise notamment à répondre aux préoccupations en matière de protection des données à caractère personnel, un droit fondamental qui, après l'entrée en vigueur du traité de Lisbonne, a acquis encore plus d'importance dans le cadre juridique de l'Union européenne.

5. La proposition souligne l'importance de la protection des données en renvoyant explicitement aux articles pertinents des traités et d'autres instruments internationaux et en reconnaissant sa nature de droit fondamental. Cependant, elle n'envisage pas de se fonder sur l'article 16 du TFUE, et ce, en dépit du fait que l'article 1, paragraphe 1, de l'accord proposé, a pour principal objet un niveau élevé de protection des données. À cet égard, le CEPD réitère que cet accord ne concerne pas seulement l'échange de données à caractère personnel, mais également la protection de ces données. L'article 16 du TFUE n'est donc pas moins pertinent que les articles 82 et 87 du TFUE concernant la coopération judiciaire et policière qui ont été choisis comme fondement juridique.

6. La proposition relève de la procédure de l'article 218, paragraphe 6, du TFUE. En vertu de cette procédure, le Conseil ne peut adopter une décision autorisant la conclusion de l'accord qu'après avoir obtenu l'approbation du Parlement européen. Cette proposition aura donc une valeur de test pour l'application des nouvelles procédures de Lisbonne à un accord international relatif à la protection des données à caractère personnel. Le succès des futures négociations dépendra de la définition satisfaisante des principes et des garanties de protection des données dans cet accord.

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] SWIFT est une société de droit belge qui fournit des services de messagerie aux établissement financiers du monde entier. Depuis 2001, le Trésor américain adresse des injonctions administratives à SWIFT afin d'accéder à certaines données à caractère personnel concernant des transactions financières, qui sont copiées sur un serveur situé sur le territoire des États-Unis.

7. Dans ce cadre, le CEPD souligne l'importance des négociations en vue d'un accord entre l'Union européenne et les États-Unis d'Amérique sur la protection des données à caractère personnel lorsqu'elles sont transférées et traitées aux fins de prévenir les infractions pénales, dont les actes terroristes, d'enquêter en la matière, de les détecter ou de les poursuivre dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale. Le projet de mandat pour entamer ces négociations a été adopté par la Commission le 26 mai 2010. Lors de la présentation de ce projet de mandat, la Commission a insisté sur la nécessité d'un accord solide relatif à la protection des données à caractère personnel ([1]).

8. Dans ce contexte, le CEPD recommande d'ajouter à la proposition actuelle un lien solide avec les négociations avec les États-Unis sur ce cadre général transatlantique de protection des données. Il faudra veiller à ce que ces critères s'appliquent également à l'accord TFTP II. Le CEPD recommande d'inclure cette condition dans l'accord actuel, ou du moins de convenir avec le gouvernement des États-Unis qu'un futur accord possible sur la protection des données couvrirait les échanges prévus dans la présente proposition.

9. Enfin, le CEPD participe activement aux prises de position du groupe de travail de «l'article 29» sur la protection des données et du groupe de travail sur la police et la justice. Outre les points déterminés ou à déterminer dans ces prises de position, le présent avis analyse la proposition actuelle en s'appuyant sur de précédentes observations du CEPD concernant l'accord intérimaire et les négociations en cours avec les États-Unis.

II. ANALYSE DE LA PROPOSITION

II.1. La proposition contient certaines améliorations

10. Le CEPD reconnaît que cette proposition envisage certaines améliorations substantielles par rapport à l'accord intérimaire TFTP I, telles que:

— L'exclusion des données SEPA. La proposition prévoit explicitement que les demandes du Trésor américain ne portent pas sur des données liées à l'espace unique de paiements en euros (article 4, paragraphe 2, point d).

— La définition du terrorisme. L'article 2 de la proposition s'inspire de la définition du terrorisme selon l'approche de l'article premier de la directive-cadre 2002/475/JAI du Conseil ([2]).

11. En outre, suite aux demandes du Parlement européen et des autorités européennes chargées de la protection des données, la proposition énonce une série de dispositions (articles 14 à 18) portant sur les droits des personnes concernées, tels que le droit d'être informé, le droit d'accès, le droit de rectification, d'effacement ou de verrouillage, ainsi que le droit de recours. Toutefois, la force exécutoire concrète de ces dispositions et les procédures à suivre par les citoyens ou résidents non américains ne sont toujours pas clairement établies (voir le paragraphe II.2.3 ci-dessous).

II.2. Mais d'autres points restent à améliorer

12. Le CEPD partage sans réserve la nécessité de garantir, comme envisagé à l'article 1, paragraphe 1, de la proposition, le respect intégral de la vie privée et de la protection des données à caractère personnel. Dans cette optique, le CEPD fait observer qu'il reste certaines questions ouvertes auxquelles il convient de répondre et des éléments clés à améliorer afin de satisfaire aux conditions du cadre juridique de l'Union européenne sur la protection des données à caractère personnel.

II.2.1. *Le traitement envisagé des données à caractère personnel est-il réellement nécessaire et proportionné?*

13. Le CEPD est pleinement conscient que la lutte contre le terrorisme et le financement du terrorisme peuvent exiger des restrictions au droit à la protection des données à caractère personnel ainsi qu'aux dispositions du secret bancaire. Cela est déjà le cas dans un ensemble d'instruments européens ([3]) qui contiennent un nombre de mesures visant à combattre l'utilisation abusive du système financier aux fins du blanchiment de capitaux et du financement du terrorisme. Ces instruments contiennent également des dispositions spécifiques qui autorisent l'échange d'informations avec les autorités de pays tiers ainsi que des garanties de la protection des données à caractère personnel, conformément à la directive 95/46/CE.

14. En outre, l'accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire permet explicitement l'échange d'informations relatives aux comptes bancaires et aux transactions financières entre les autorités policières et judiciaires, et il prévoit des conditions et des restrictions en ce qui concerne cet échange. Au niveau international également, ce qu'il est convenu d'appeler les principes d'Egmont ([4]) établissent la base de l'échange international d'informations relatives aux transactions financières entre les cellules de renseignement financier, tout en fixant des restrictions et des garanties en ce qui concerne l'utilisation des données échangées. En outre, les instruments concernant l'échange de données entre les États-Unis, Europol et Eurojust sont déjà en place, garantissant à la fois l'échange d'informations et la protection des données à caractère personnel.

([1]) Voir le communiqué de presse, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/609&format=HTML&aged=0&language=FR&guiLanguage=fr

([2]) Décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme, (JO L 164 du 22.6.2002, p. 3).

([3]) Notamment la directive 2005/60/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, ainsi que le règlement (CE) nº 1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds.

([4]) http://www.egmontgroup.org/library/download/5

15. Dans ce contexte, la proposition de la Commission souligne l'intérêt du programme TFTP, tel que présenté par le Trésor américain et les rapports de la personnalité éminente. Toutefois, la condition visée à l'article 8 de la CEDH afin de justifier l'atteinte à la vie privée est plus une «nécessité» qu'un «intérêt».

16. Selon le CEPD, il convient d'apporter suffisamment de preuves de la réelle valeur ajoutée de cet accord au regard des instruments déjà existants, ou, en d'autres termes, de déterminer dans quelle mesure l'accord est réellement nécessaire afin de parvenir à des résultats impossibles à obtenir en utilisant des instruments moins intrusifs pour la vie privée, tels que ceux qui existent déjà dans le cadre européen et international. Selon le CEPD, cette valeur ajoutée doit être clairement établie, en tant que condition préalable à tout accord avec les États-Unis sur l'échange de données financières, compte tenu également de la nature intrusive de l'accord (voir également les paragraphes 18 à 22 sur la proportionnalité).

17. Le CEPD n'est pas en mesure d'apprécier la nécessité de cet accord. Toutefois, même si la nécessité de l'accord venait à être démontrée, il n'en reste pas moins que d'autres points méritent d'être examinés par les négociateurs.

18. Le principe de la proportionnalité est également le principal critère à prendre en considération aux fins de l'appréciation du volume de données à caractère personnel transférées et de leur durée de conservation. L'article 4 de la proposition limite la portée des demandes américaines. Cependant, la proposition maintient que les données à caractère personnel seront transférées en masse aux autorités américaines, puis conservées en principe pendant une durée de 5 ans, sans considération du fait qu'elles aient été extraites ou non ou qu'il existe un lien avéré avec une enquête ou des poursuites bien précises.

Transferts en masse

19. Malgré les demandes du Parlement européen et des autorités européennes chargées de la protection des données, la proposition est toujours fondée sur le principe selon lequel les données à caractère personnel seront transmises en masse au Trésor américain. Concernant ce point, il est important de préciser que le fait que le système actuel de SWIFT ne permette pas d'effectuer une recherche ciblée ne peut être considéré comme une justification suffisante pour rendre les transferts de données en masse légitimes au regard de la loi de l'UE relative à la protection des données.

20. Par conséquent, le CEPD estime qu'il convient de trouver des solutions afin de veiller au remplacement des transferts en masse par des mécanismes permettant de filtrer les données de transactions financières dans l'UE, et de veiller à ce que seules les données pertinentes et nécessaires soient envoyées aux autorités américaines. Si de telles solutions ne peuvent être trouvées dans l'immédiat, dans ce cas l'accord devrait en tout état de cause définir une courte période transitionnelle après laquelle les transferts en masse ne seront plus autorisés.

Période de conservation

21. En ce qui concerne la période de conservation, le CEPD reconnaît que la proposition fixe correctement des délais de conservation maximaux ainsi que des mécanismes pour veiller à ce que les données à caractère personnel soient effacées lorsqu'elles ne sont plus nécessaires. Cependant, les dispositions de l'article 6 de la proposition concernant les données non extraites semblent aller dans la direction opposée. Tout d'abord, la notion de «données non extraites» ne tombe pas sous le sens et devrait donc être expliquée. Deuxièmement, les raisons pour lesquelles il est nécessaire de conserver des données non extraites pendant une durée de 5 ans ne sont pas exposées.

22. Le CEPD reconnaît en tous points la nécessité de garantir que les données à caractère personnel nécessaires dans le cadre d'enquêtes ou de poursuites liées à un acte terroriste en particulier puissent être consultées, traitées et conservées aussi longtemps que nécessaire, dans certains cas même au-delà de 5 ans, certaines données à caractère personnel pouvant être nécessaires dans des enquêtes ou des procédures judiciaires longues. Cependant, si l'on part du principe que les données non extraites sont des données qui ont été transférées en masse et auxquelles il n'a pas été accédé ou qui n'ont pas été utilisées dans le cadre d'enquêtes ou de poursuites bien précises, la période de conservation autorisée devrait être bien plus limitée. Dans cette perspective, il est utile de souligner que la Cour constitutionnelle fédérale allemande a jugé, en ce qui concerne la conservation de données de télécommunications, qu'une période de conservation de 6 mois était déjà très longue et qu'elle devait être justifiée de manière appropriée ([1]). La Cour constitutionnelle semblait considérer cette période de 6 mois comme étant la période maximale autorisée pour des données ne se rapportant à aucune enquête bien précise.

II.2.2. *La proposition garantit-elle un contrôle judiciaire?*

23. Selon le mandat de négociation, il incombe à une autorité judiciaire publique de recevoir les demandes émanant du Trésor américain, d'apprécier leur conformité à l'accord et, le cas échéant, d'exiger du fournisseur qu'il transfère les données sur la base d'un système d'exportation (système «push»). Le Parlement européen comme le CEPD a approuvé cette approche, qui représente une garantie cruciale — et conforme aux constitutions nationales et aux systèmes juridiques des États membres — assurant des transferts de données licites et équilibrés ainsi qu'une surveillance indépendante.

([1]) Arrêt du 2 mars 2010.

24. Toutefois, la proposition confie cette mission à Europol, une agence de l'Union européenne qui a pour objectif de prévenir la criminalité organisée, le terrorisme et d'autres formes graves de criminalité, affectant deux États membres ou plus et de lutter contre ces phénomènes ([1]). Europol n'est de toute évidence pas une autorité judiciaire.

25. En outre, Europol a des intérêts particuliers dans l'échange de données à caractère personnel, sur la base de l'accord proposé. L'article 10 de la proposition habilite Europol à demander une recherche d'informations pertinentes obtenues dans le cadre du TFTP, s'il établit qu'il y a lieu de penser qu'une personne ou une entité a un lien avec le terrorisme. Il est difficile de concilier cette compétence d'Europol, qui peut s'avérer essentielle à la bonne exécution de la mission d'Europol et qui requiert de bonnes relations avec le Trésor américain, avec la mission d'Europol, qui consiste à garantir un contrôle indépendant.

26. En outre, le CEPD se demande dans quelle mesure le cadre juridique actuel confie à Europol — surtout sans modifier son fondement juridique conformément à la procédure ordinaire établie par le traité de Lisbonne — la mission visant à faire en sorte qu'une demande administrative émanant d'un pays tiers devienne «contraignante» (article 4, paragraphe 5) pour une société privée, qui aura dès lors «le pouvoir et le devoir» de fournir des données à ce pays tiers. Dans ce contexte, il est utile de noter qu'en l'état actuel du droit européen, il n'est pas évident de savoir si une décision d'Europol vis-à-vis d'une entreprise privée ferait l'objet d'un contrôle judiciaire par la Cour européenne de justice.

27. Dans ce contexte, le CEPD réitère sa position selon laquelle, également en vue de respecter le mandat de négociation et le cadre juridique actuel de l'UE, la mission qui consiste à apprécier les demandes du Trésor américain devrait être confiée à une autorité judiciaire publique.

II.2.3. *La proposition confère-t-elle des droits (et une protection) exécutoires aux personnes concernées?*

28. Comme déjà mentionné dans l'introduction du présent avis, la proposition énonce un ensemble de droits des personnes concernées, tels que le droit d'être informé, le droit d'accès, le droit de rectification, d'effacement ou de verrouillage, ainsi que le droit de recours. Cependant, il est important, d'une part, d'améliorer certains éléments de ces dispositions et, d'autre part, de garantir leur réelle force exécutoire.

29. En ce qui concerne le droit d'accès à ses propres données à caractère personnel, l'accord détermine un ensemble de restrictions. Le CEPD reconnaît que, notamment dans le contexte de la lutte contre le terrorisme, des restrictions aux droits des personnes concernées peuvent être mises en place dès lors qu'elles sont nécessaires. Toutefois, la proposition devrait clairement indiquer, alors que la divulgation à une personne de ses données à caractère personnel peut très bien se limiter aux circonstances mentionnées à l'article 15, paragraphe 2, que la divulgation de ces informations aux autorités nationales européennes chargées de la protection des données doit dans tous les cas être possible, afin de permettre à ces autorités de mener à bien leur mission de contrôle. Évidemment, les autorités chargées de la protection des données seront liées par une obligation de confidentialité dans l'exercice de leur mission et ne divulgueront pas les données à la personne concernée, aussi longtemps que les conditions d'une exception subsistent.

30. En ce qui concerne le droit de rectification, l'article 17, paragraphe 2, dispose que «chaque Partie informe, si possible, l'autre Partie si elle se rend compte que des informations potentiellement importantes qu'elle a transmises à l'autre Partie ou qu'elle a reçues de cette autre Partie au titre du présent accord sont inexactes ou sujettes à caution». Le CEPD estime que l'obligation de rectifier des données inexactes ou sujettes à caution est une garantie fondamentale non seulement pour la personne concernée, mais également pour l'efficacité de l'action des autorités policières et judiciaires. Dans cette perspective, les autorités qui échangent des données devraient mettre en place des mécanismes afin de veiller à ce que cette rectification soit toujours possible, et les termes «si possible» devraient dès lors être supprimés de la proposition.

31. Cependant, le CEPD est avant tout préoccupé par la réelle force exécutoire de ces droits. D'une part, pour des raisons de sécurité juridique et de transparence, la proposition devrait préciser plus en détail quelles sont les procédures concrètes que les personnes concernées peuvent suivre afin de faire valoir les droits reconnus par l'accord, dans l'UE comme aux États-Unis.

32. Par ailleurs, l'article 20, paragraphe 1, dispose explicitement et clairement que l'accord «ne crée ni ne confère aucun droit ou avantage pour toute personne ou entité, privée ou publique». Le CEPD fait observer que cette disposition semble annuler ou tout au moins remettre en cause l'effet contraignant des dispositions de l'accord qui garantissent les droits des personnes concernées, qui ne sont actuellement ni reconnus ni applicables en vertu du droit américain, notamment lorsque les personnes concernées ne sont ni des citoyens américains ni des résidents permanents aux États-Unis. Par exemple, le US Privacy Act (loi américaine sur la protection de la vie privée) prévoit un droit d'accès aux données personnelles, assorti de réserves, qui prévaut sur le droit général d'accès conféré au grand public par le US Freedom of Information Act (loi américaine relative à la liberté de l'information). Cependant, le US Privacy Act indique clairement qu'une demande d'accès à ses propres données est seulement possible pour «un citoyen des États-Unis ou un étranger légalement admis en tant que résident permanent» ([2]).

([1]) Voir, par exemple, l'article 3 de la décision du Conseil 2009/371/JAI portant création de l'Office européen de police (Europol), JO L 121 du 15.5.2009, p. 37.

([2]) Les informations disponibles sur le site internet du Trésor américain le confirment: «[…] lorsque vous présentez une demande de notification ou d'accès à des données, vous devez: [...] préciser que vous êtes un citoyen des États-Unis ou un étranger légalement admis en tant que résident permanent aux États-Unis; [...]», http://www.treas.gov/foia/how-to.html (dernier accès le 21 juin 2010).

33. Le CEPD recommande dès lors que le libellé actuel de l'article 20, paragraphe 1, soit réexaminé afin de veiller à ce que les droits conférés par la proposition soient clairement énoncés et applicables, y compris sur le territoire américain.

II.2.4. *La proposition garantit-elle un contrôle et un suivi indépendants satisfaisants?*

34. L'article 12 de la proposition prévoit plusieurs niveaux de contrôle des conditions et garanties établies par l'accord. Des «contrôleurs indépendants» surveilleront en temps réel et rétrospectivement les recherches mises en place par le Trésor américain. En outre, «une personnalité indépendante désignée par la Commission européenne» effectuera un suivi régulier du premier niveau de contrôle, y compris de son indépendance. Il convient de préciser quelles seront les tâches de cette personnalité indépendante, comment il sera garanti qu'elle s'acquitte bel et bien de ses tâches et de qui elle relèvera.

35. L'article 13 prévoit également un mécanisme de réexamen conjoint qui a lieu après un délai de 6 mois, puis sur une base régulière. Ce réexamen conjoint sera effectué par une délégation UE-US conjointe, comprenant pour la délégation européenne des représentants de deux autorités chargées de la protection des données, et donnera lieu à un rapport que la Commission présentera au Parlement européen et au Conseil.

36. Le CEPD souligne que le contrôle indépendant est un élément clé du droit à la protection des données à caractère personnel, comme le confirme l'article 16 du TFUE et l'article 8 de la Charte des droits fondamentaux de l'Union. Récemment, la Cour de justice a établi des critères stricts d'indépendance dans son arrêt du 9 mars 2010, Commission/Allemagne ([1]). Ces mêmes critères stricts ne peuvent évidemment pas être imposés à des pays tiers, mais il va également de soi qu'il ne peut y avoir de protection adéquate des données à caractère personnel ([2]) en l'absence de garanties suffisantes de contrôle indépendant. Il s'agit également d'une condition pour les accords internationaux avec des pays dont l'ordre juridique n'établit pas la nécessité d'un contrôle par une autorité indépendante.

37. Dans ce contexte, il est crucial, au moins, que les modalités du contrôle et du réexamen conjoint, ainsi que les compétences et les garanties d'indépendance des personnes participant au contrôle soient clairement définies dans l'accord plutôt que d'être «réexaminées conjointement» ou déterminées à un stade ultérieur par les parties. Il est notamment important de veiller à ce que la personnalité désignée par la Commission européenne et les représentants des autorités européennes chargées de la protection des données soient mis en mesure d'agir indépendamment et de mener à bien leurs missions de contrôle.

38. En outre, la proposition doit non seulement fixer la date du premier réexamen conjoint, qui doit se tenir après un délai de 6 mois, mais également la fréquence des réexamens suivants, qui peuvent par exemple avoir lieu tous les ans. Le CEPD recommande également d'établir un lien entre le résultat de ces réexamens conjoints et la durée de l'accord.

39. Dans ce contexte, le CEPD insiste sur le fait qu'une clause de suspension est souhaitable, à la lumière également de l'éventuelle disponibilité de solutions plus ciblées sur le long terme. Une clause de suspension permettrait également de garantir que les efforts nécessaires sont consacrés à la mise en place de telles solutions, et de ce fait, il n'y aurait plus aucune raison d'envoyer des données en masse au Trésor américain.

40. Afin d'améliorer l'efficacité du contrôle et du réexamen conjoint, les informations et les données pertinentes sur le nombre de demandes d'accès et de recours, de suivi possible (effacement, rectification, etc.), ainsi que le nombre de décisions restreignant les droits des personnes concernées doivent être disponibles. Dans le même esprit, dans la mesure où le réexamen est concerné, des informations doivent être disponibles et communiquées sur la quantité de messages auxquels le Trésor américain a «accédé» mais également sur le nombre de messages «fournis» au Trésor américain. Cela doit être précisé dans l'accord.

41. En outre, les compétences des autorités européennes chargées de la protection des données ne doivent en aucun cas être limitées par cette proposition. Dans cette perspective, le CEPD fait observer que la proposition ne va pas dans le bon sens par rapport à l'accord intérimaire TFTP. En effet, alors que l'accord précédent disposait dans son préambule que «le présent accord ne déroge pas à la compétence qu'ont les autorités des États membres responsables de la protection des données de protéger les particuliers à l'égard du traitement de leurs données à caractère personnel», la proposition mentionne désormais «le contrôle des autorités compétentes chargées de la protection des données dans le respect des dispositions spécifiques du présent accord». Le CEPD recommande donc que la proposition indique clairement que l'accord ne déroge pas à la compétence des autorités européennes chargées de la protection des données et qu'il ne la limite pas.

III. **CONCLUSIONS**

42. Le CEPD reconnaît que cette proposition envisage certaines améliorations substantielles par rapport à l'accord intérimaire TFTP I, telles que l'exclusion de données SEPA, une définition plus limitée du terrorisme, ainsi que des dispositions plus détaillées sur les droits des personnes concernées.

([1]) Affaire C-518/07, non encore publiée au Recueil.

([2]) L'article 8 de la proposition d'accord dispose que le Trésor américain est censé garantir un niveau de protection approprié.

43. Le CEPD fait cependant observer qu'une condition préalable essentielle à l'appréciation de la légitimité d'un nouvel accord TFTP doit être satisfaite. La nécessité du mécanisme doit être établie par rapport aux instruments européens et internationaux déjà existants.

44. Si tel était le cas, le CEPD souligne qu'il reste certaines questions ouvertes auxquelles il convient de répondre et des éléments clés à améliorer afin de satisfaire aux conditions du cadre juridique de l'Union européenne sur la protection des données à caractère personnel, tels que:

— veiller au remplacement des transferts de masse par des mécanismes permettant de filtrer les données de transactions financières dans l'UE, et veiller à ce que seules les données pertinentes et nécessaires soient envoyées aux autorités américaines;

— réduire de manière considérable la période de conservation des données non extraites;

— confier à une autorité judiciaire publique l'appréciation des demandes du Trésor américain, conformément au mandat de négociation et à l'actuel cadre juridique de l'UE;

— veiller à ce que les droits de la personne concernée conférés par la proposition soient clairement énoncés et applicables, y compris sur le territoire américain;

— améliorer les mécanismes de contrôle indépendant et de suivi:

i) en veillant à ce que les missions et le rôle de la personnalité désignée par la Commission européenne et des représentants des autorités européennes chargées de la protection des données soient bien définis et à ce qu'ils soient mis en mesure d'agir indépendamment et de mener à bien leurs missions de contrôle;

ii) en veillant à ce que des réexamens conjoints se tiennent régulièrement et que leur résultat soit lié à la durée de l'accord au moyen d'une clause de suspension;

iii) en transmettant les informations disponibles à des contrôleurs indépendants et des autorités chargées de la protection des données;

iv) en évitant que l'accord limite les compétences des autorités européennes chargées de la protection des données;

— mentionner le présent avis dans les considérants de la proposition.

Fait à Bruxelles, le 22 juin 2010.

Peter HUSTINX

Contrôleur européen de la protection des données