Observations sur la communication de la Commission au Parlement européen, au Conseil, au Conseil économique et social européen et au Comité des régions du 13 juillet 2011: «Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme»

1. *Contexte général et origine du système*

Il est rappelé dans la communication que la principale raison du développement d'un système européen de surveillance du financement du terrorisme («SSFT») trouve son origine dans l'actuel accord TFTP américain (et notamment son article 11) et dans la décision du Conseil du 13 juillet 2010 («la décision»). Actuellement, en application du TFTP, des données sont transférées massivement aux États-Unis, afin d'y être stockées et filtrées en fonction des demandes du département du Trésor américain. Ce système a suscité de vives critiques, surtout de la part du Parlement européen (et bien évidemment du CEPD et du groupe de travail «Article 29»), notamment en ce qui concerne la nécessité et la proportionnalité des transferts «massifs» de données.

L'accord envisage une possible *«coopération avec un futur système européen équivalent»* au cas où la Commission, après avoir réalisé sa propre étude, déciderait de mettre en place un système européen *«permettant un transfert plus ciblé de données»*.

Dans la décision, le Conseil a consenti à la conclusion d'un accord entre l'Union européenne et les États-Unis d'Amérique tout en invitant la Commission à soumettre au Parlement européen et au Conseil un cadre légal et technique pour l'extraction des données sur le territoire de l'UE. En outre, en donnant son accord à la conclusion de l'accord du 8 juillet 2010, le Parlement européen a explicitement pris acte de l'engagement du Conseil et de la Commission de mettre en place le cadre légal et technique permettant *l'extraction des données* sur le territoire de l'UE. Cet engagement permettrait de garantir à moyen terme la fin des transferts massifs de données aux autorités américaines.

Le CEPD est favorable à ce que les données soient au préalable filtrées dans l'Union européenne dans la mesure où cela permettrait de ne pas transférer massivement des données à un pays tiers. Cependant, la communication va au-delà de la finalité déclarée de filtrer les données dans l'UE, étant donné qu'elle indique clairement que le *«système ne doit pas être établi à la seule fin de fournir des informations utiles aux autorités américaines»*, dans la mesure où *«les résultats que le système permettra d'obtenir revêtiront également un réel intérêt»* pour les autorités des États membres[1].

La communication semble donc légitimer la mise en place d'un tout nouveau SSFT, dans un contexte spécifique à l'Union, sur la base de l'accord TFTP existant. En d'autres termes, la communication semble justifier l'introduction d'un nouveau système portant atteinte à la vie privée des citoyens européens dans l'intérêt des autorités des États membres de l'Union en se

[1] Communication, point 3, p. 4. .

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 63
Courriel: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax : 02-283 19 50

servant de l'évaluation de l'utilité d'un système conçu et mis en place pour permettre aux autorités américaines de poursuivre leur propre enquête sur le terrorisme.

Le CEPD émet de sérieux doutes sur cette approche qui ne semble pas respecter les principes de nécessité et de proportionnalité (comme détaillé ci-dessous).

2. *Nécessité et proportionnalité*

Nécessité

La communication mentionne à plusieurs reprises la «valeur ajoutée» ou «l'intérêt» du TFTP américain, sans faire référence à aucune analyse de l'efficacité d'instruments existants, y compris les cellules de renseignement financier (CRF) qui jouent déjà un rôle spécifique par rapport au financement du terrorisme, étant donné qu'elles coopèrent au sein du groupe Egmont pour échanger des données de renseignement financier.

Une évaluation positive du TFTP américain, qui semblerait satisfaire les besoins des autorités américaines, ne peut être transposée en tant que telle dans le cadre interne européen, sans une analyse approfondie des instruments existants dont disposent les services d'enquête européens et – au cas où ces instruments ne seraient pas pleinement satisfaisants – de l'éventuelle nécessité d'un nouveau système dans le contexte spécifique de l'Union.

Le CEPD recommande vivement qu'une telle analyse approfondie soit réalisée dans le cadre de l'analyse d'impact. Cette analyse devrait avant tout se concentrer sur les conditions et les garanties nécessaires à la mise en place d'un système de filtrage au sein de l'Union européenne, dans le cadre de l'accord TFTP avec les États-Unis. Dans un deuxième temps seulement, la nécessité d'un SSFT européen serait analysée, en tenant compte des mécanismes existants basés sur le cadre européen actuel.

Dans de nombreux avis et de nombreuses observations, le CEPD a prôné la nécessité d'une évaluation de l'ensemble des instruments existants dans le domaine de la liberté, de la sécurité et de la justice avant d'en proposer de nouveaux[2]. Il est crucial d'évaluer l'efficacité des mesures existantes tout en tenant compte de l'incidence des nouvelles mesures envisagées sur la vie privée et cette évaluation devrait jouer un rôle essentiel dans les mesures prises par l'Union européenne dans ce domaine, conformément à l'approche exposée dans le programme de Stockholm.

Proportionnalité

Comme indiqué ci-dessus, le principal problème de proportionnalité concernant actuellement le TFTP concerne la collecte de données en masse par les autorités américaines à la source du traitement, c'est-à-dire à partir de la société de transactions financières sur le territoire européen. Le TFTP américain serait basé sur un cadre solide et bien développé de protection des données (comme indiqué p. 5 de la communication) ainsi que sur la limitation du champ d'application à la lutte contre le terrorisme et son financement (voir p. 3 de la communication). Cependant, ces éléments en tant que tels ne «contrebalancent pas les effets du transfert massif de données», contrairement à ce qui est allégué dans la communication

[2] Voir par exemple l'avis du 30 septembre 2010 sur la «Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice», et l'avis du 24 novembre 2010 sur la communication de la Commission au Parlement européen et au Conseil – «La politique antiterroriste de l'UE: principales réalisations et défis à venir».

(p. 3). Ils ne satisfont pas aux exigences préliminaires de la proportionnalité telles qu'exposées ci-dessus.

Compte tenu de cette grave lacune que présente le TFTP actuel, la Commission ne devrait pas se fier à l'analyse de proportionnalité réalisée dans le cadre de ce dernier. Le CEPD recommande donc vivement qu'une analyse de proportionnalité approfondie et indépendante soit réalisée concernant le SSFT proposé dans l'analyse d'impact. Elle devrait examiner les modalités envisagées de l'extraction des données sur le territoire de l'UE, notamment quelles sont les données qui sont supposées être transférées de la société de transactions financières à l'autorité censée mener l'enquête et de quelle manière elles doivent être transférées. L'analyse doit évaluer les façons de limiter le traitement de données à caractère personnel dans ce contexte. L'analyse d'impact devrait également, dans un point séparé, examiner la proportionnalité que présente la création d'un nouveau SSFT européen par rapport à l'objectif de la lutte contre le financement du terrorisme, comme établi dans la communication (p. 3).

3. Garanties procédurales

Le CEPD souhaiterait également mettre en évidence le manque de clarté des garanties procédurales envisagées dans les trois options pour le SSFT qui sont décrites dans la communication. La communication établit une distinction entre plusieurs fonctions qui doivent être mises en œuvre afin de mettre en place la surveillance du financement du terrorisme.

La première étape est la préparation et l'envoi, par les autorités, des «demandes» de transmission de données brutes aux prestataires désignés de services de messagerie financière. Ces demandes doivent ensuite être contrôlées et autorisées. Dans la communication, la Commission envisage deux options en ce qui concerne l'origine des demandes: elles proviennent soit d'une «unité centrale européenne du SSFT» (options 1 et 2), soit du «service de coordination modernisé des cellules de renseignement financier» (option 3). La terminologie employée pour indiquer quel type de garanties procédurales doit être appliqué lors de la phase des «demandes» dans les trois options reste vague. Le CEPD invite la Commission à élaborer des garanties solides et spécifiques.

Cet aspect est d'autant plus important qu'il constitue une différence fondamentale avec le système TFTP américain actuel. Alors que dans ce dernier, les demandes (ordres de production) émanent du département du Trésor américain et doivent respecter les critères établis à l'article 4 de l'accord (spécificité de la demande, nécessité, adaptation étroite, exclusion des données SEPA), dans les trois options envisagées par la communication, il n'y a aucune trace des critères valables (niveau de suspicion, existence d'autres éléments de preuve, etc…) sur la base desquels toute demande d'extraction des données devrait être initialement vérifiée.

Par exemple, le texte de la communication mentionne que la préparation des demandes dans le cadre de l'option 1 *«pourrait se faire en concertation avec les autorités responsables des États membres»*, que les États membres se trouveraient dans l'obligation de *«partager des informations»* avec l'unité centrale du SSFT afin de motiver la demande et d'établir le lien entre la demande et le terrorisme, ou de faire valider «préalablement» leur demande par les autorités nationales. Il est ensuite indiqué que ces autorités pourraient par exemple être les juges d'instruction ou les procureurs chargés de la lutte contre le terrorisme au niveau national. Dans ce cas, aucun renseignement supplémentaire ne devrait être communiqué à l'unité centrale européenne du SSFT.

Dans ce scénario cependant, les éléments procéduraux ou valables qui doivent être évalués avant que tout type de recherche soit autorisé ne sont pas mentionnés. Le fait que la validation préalable de la demande par les autorités judiciaires – qui prennent vraisemblablement part aux enquêtes sur le terrorisme – soit mentionnée comme étant une des possibilités envisagées par l'option 1 soulève une question essentielle: le CEPD émet de sérieux doutes quant à la question de savoir si toute demande liée à une enquête sur le terrorisme pourrait être justifiée autrement que sous le contrôle des autorités judiciaires. Toute demande entraînerait une grave atteinte à la protection des données à caractère personnel des citoyens européens qui n'ont rien à voir avec des activités terroristes; il convient donc de souligner qu'une telle atteinte devrait uniquement être autorisée avec l'approbation des autorités judiciaires des différents États membres sur la base de critères valables.

Comme souligné ci-dessus, la communication reste vague à ce sujet. Le CEPD encourage donc vivement la Commission à préciser, surtout dans le cadre d'un service centralisé de coordination et d'analyse de l'UE, quels sont les critères valables qui doivent être respectés pour l'envoi initial des demandes, et à réfléchir à l'importance des garanties procédurales offertes par les différentes législations de procédure pénale nationale des États membres.

La fonction des CRF dans la proposition de «forum modernisé des CRF» (option 3 de la communication) devrait également être précisée, et comparée aux compétences actuelles des CRF. Pour les mêmes raisons qui sont susmentionnées, des conditions claires de collaboration avec les autorités judiciaires devraient être analysées et motivées en vue de garantir le respect des garanties procédurales établies dans les systèmes judiciaires des différents États membres.

4. Mécanismes de surveillance

En ce qui concerne les mécanismes de surveillance, la communication mentionne également le rôle que pourraient jouer des «contrôleurs». On ne sait pas précisément dans quelle mesure le rôle de ces contrôleurs serait défini en analogie avec leur rôle dans l'accord TFTP américain, et si une surveillance par des acteurs privés est envisagée. Nous estimons qu'un tel mécanisme impliquant des acteurs privés ne devrait pas être transposé dans le cadre de l'UE. Le cadre de l'UE nécessite une surveillance institutionnalisée et tout rôle spécifique conféré aux contrôleurs ne devrait en aucun cas remplacer les garanties judiciaires susmentionnées et le rôle de surveillance des autorités chargées de la protection des données.

5. Utilisation de structures existantes

La communication approuve l'utilisation de structures qui existent déjà (p. 6). Cet aspect soulève des questions d'interopérabilité et présente des risques de détournement d'usage. Le fait qu'une structure existante soit utilisée ne devrait pas permettre d'échanger des données avec d'autres bases de données. Il doit être rappelé qu'aucune interconnexion de bases de données ne devrait être établie sans une base claire et légitime[3]. En outre, les données à caractère personnel ne devraient pas être utilisées à des fins s'écartant de celles strictement

[3] Voir à cet égard les observations du CEPD du 10 mars 2006 relatives à la communication de la Commission sur l'interopérabilité des bases de données européennes, disponibles à l'adresse www.edps.europa.eu: *Quand on parle d'interopérabilité, il ne s'agit pas seulement de l'utilisation en commun de systèmes d'information à grande échelle, mais également de possibilités d'accès aux données, d'échange de données ou même de fusion de bases de données. Ceci est regrettable, dans la mesure où des types d'interopérabilité différents requièrent des garanties et des conditions différentes. Tel est notamment le cas lorsque la notion d'interopérabilité sert de point de départ à d'autres mesures proposées visant à faciliter l'échange d'informations. Dans son avis sur le principe de disponibilité, le CEPD a souligné que bien qu'il n'entraîne pas la création de nouvelles bases de données, ce principe suscitera inévitablement une nouvelle manière d'utiliser les bases de données existantes, puisqu'il offre de nouvelles possibilités d'accès à ces bases.*

définies dans le système, lesquelles, selon le point de vue du CEPD, devraient se limiter strictement à la lutte contre le terrorisme et son financement: l'utilisation d'une structure existante ne garantit pas en soi le respect du principe de limitation de la finalité.

Conséquences d'un possible SSFT européen par rapport au TFTP américain existant

Le TFTP américain a été instauré par les autorités américaines afin d'accéder plus rapidement et plus efficacement aux données financières, plutôt que de suivre la procédure prévue dans les instruments existants, notamment l'accord sur l'entraide judiciaire entre l'Union européenne et les États-Unis[4] et les mesures mises en place par le groupe d'action financière (GAFI), comprenant les CRF nationales. Le TFTP américain permet aux autorités américaines d'accéder à un vaste ensemble de données et d'effectuer elles-mêmes des recherches selon leurs propres critères. Il s'agit d'un des principaux problèmes sur le plan de la protection des données, étant donné que la condition de la proportionnalité n'est pas remplie selon les critères européens, comme l'ont déjà souligné le CEPD et le groupe de travail «Article 29» dans de précédents avis[5].

Si le filtrage des données est effectué au sein de l'UE dans le cadre du SSFT, selon des critères qui devraient être particulièrement stricts (afin de respecter les conditions de nécessité et de proportionnalité), les données envoyées aux États-Unis seraient de ce fait limitées. Cette condition est essentielle pour se conformer aux exigences européennes en matière de protection des données, même si les données ne répondraient pas totalement aux (larges) demandes des autorités américaines.

L'incidence de cette modification sur la motivation générale de l'accord TFTP américain n'est pas examinée dans la communication, bien que ce point précis soit soulevé à l'article 12, paragraphe 3, de l'accord. Le CEPD invite la Commission à mener une réflexion sur le réel impact qu'un SSFT européen aurait sur la mise en œuvre actuelle du TFTP américain. La Commission devrait vérifier si une révision anticipée de l'accord est nécessaire afin d'adapter les règles régissant le transfert Union européenne-États-Unis de données de messagerie financière au nouveau système envisagé.

Le CEPD attend que la Commission prépare une analyse approfondie sur l'analyse d'impact et qu'elle le consulte à ce sujet.

Bruxelles, le 25 octobre 2011

---

[4] Décision du Conseil du 6 juin 2003 concernant la signature des accords entre l'Union européenne et les États-Unis d'Amérique sur l'extradition et l'entraide judiciaire en matière pénale; JO L 181 du 19.07.2003, p. 25

[5] Voir notamment:

- Avis du CEPD du 22 juin 2010 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), disponible à l'adresse: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-06-22_Opinion_TFTP_FR.pdf.
- Avis 10/2006 du groupe de travail «Article 29» sur le traitement de données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128, disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_fr.pdf