AVIS N° 47 / 2006 du 20 décembre 2006

N. Réf. : SA2 / A / 2006 / 045

OBJET : avis relatif à la préparation d'une convention concernant la transmission de données à caractère personnel par SWIFT à l'US Department of the Treasury (UST).

La Commission de la protection de la vie privée ;

Vu la Directive 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* (ci-après la "Directive 95/46/CE") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "Loi vie privée"), en particulier l'article 29, § 1 ;

Vu l'avis n° 37/2006 de la Commission du 27 septembre 2006 *relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST* (ci-après "l'avis SWIFT") ;

Vu l'avis n° 10/2006 du 22 novembre 2006 (WP 128) du Groupe 29 *sur le traitement des données à caractère personnel par SWIFT*[1] ;

Vu la demande d'avis de Monsieur le Premier Ministre du 31 octobre 2006, reçue le 3 novembre 2006 ;

Vu le rapport de Monsieur De Schutter ;

Emet, le 20 décembre 2006, l'avis suivant :

[1] Tel que publié sur le site Internet : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_fr.htm

A. INTRODUCTION

Suite à l'avis SWIFT n° 37/2006 du 27 septembre 2006, le Gouvernement belge a décidé d'envisager – dans le cadre d'une concertation aussi large que possible avec les Etats-Unis – des initiatives permettant de trouver une solution pour que le système juridique des Etats-Unis garantisse un niveau de protection des données à caractère personnel équivalent à celui de l'Union européenne.

Afin de pouvoir préparer un accord avec les Etats-Unis, le Premier Ministre a invité la Commission, dans une demande reçue le 3 novembre 2006, à émettre un avis sur ce que devrait contenir une convention avec les Etats-Unis et sur la forme que pourrait prendre une telle convention.

Cet avis contient un rappel (1) de quelques considérations générales importantes relatives aux actions pouvant être entreprises par le Gouvernement belge (rubrique B) et (2) au contexte européen dans lequel est opéré le transfert de données à caractère personnel à l'UST (rubrique C). L'attention se porte ensuite sur (3) le contenu (rubrique D) et (4) la forme (rubrique E) de la convention visée par le Gouvernement.

Cet avis s'inscrit dans la perspective de la "protection de données à caractère personnel", sans toutefois négliger la protection contre la terreur et le terrorisme. La Commission de la protection de la vie privée est tout à fait consciente que cette menace requiert une politique constante et ferme. Elle soutient pleinement cette approche. La Commission est convaincue que cette lutte peut être menée sans mettre en péril l'état de droit.
Sur ce point, il est choquant de constater qu'une enquête étendue, que ce soit en termes de temps et en nombre de personnes concernées, a été et est encore menée secrètement et sans contrôle démocratique. D'autant plus que nos propres services de sécurité et de justice restent privés des informations ainsi récoltées. Tout cela, en dehors de tout contrôle ou sanction judiciaire.

S'il s'avérait que des informations vitales sont présentes dans le réseau SWIFT (ce qui n'a toujours pas été démontré concrètement), le fait que les services belges (ou européens) en soient privés constitue alors une limitation grave de leurs possibilités. S'il apparaît que ce n'est pas le cas, il faut au moins tout mettre en œuvre pour faire cesser ces violations.

Le présent avis aborde des possibilités du point de vue de la protection des données. Cela n'empêche pas les démarches diplomatiques classiques que les autorités belges (ou européennes) peuvent entreprendre à l'égard de leurs collègues des Etats-Unis. Le constat que, durant des années, des données à caractère personnel de leurs citoyens aient fait l'objet, à grande échelle, d'une enquête jusqu'à nouvel ordre incontrôlée et unilatérale par les autorités d'un Etat avec lequel une collaboration étroite a lieu constitue en soi un motif de protestation justifié. Le silence pourrait être considéré comme une acceptation, voire même une approbation. La Commission de la protection de la vie privée espère que les autorités belges et européennes ne laissent subsister aucun doute quant au fait que ces infractions à la vie privée sont inacceptables.

B. APPRECIATION GENERALE

B.1. Les conclusions de l'avis n° 37/2006 du 27 septembre 2006 demeurent applicables à SWIFT

Dans son avis SWIFT, la Commission faisait une distinction entre, d'une part, les traitements commerciaux effectués par SWIFT dans le cadre du service SWIFTNet FIN et, d'autre part, la communication de données à caractère personnel à l'UST (appelée "onward transfer").

Il va de soi que la conclusion éventuelle d'un accord ou d'une convention avec les Etats-Unis en ce qui concerne la communication de données à caractère personnel à l'UST n'empêche pas que la loi belge relative à la vie privée soit applicable à SWIFT et que des actions complémentaires soient encore entreprises suite à la constatation par la Commission d'infractions à la loi belge relative à la vie privée dont SWIFT s'est rendue coupable. Le Groupe 29 a souligné, à juste titre, que pour toutes ses activités en matière de traitement de données à caractère personnel, SWIFT devait tout de même respecter les obligations auxquelles elle est soumise en vertu de la législation belge relative à la vie privée.[2]

La Commission précise qu'à ses yeux, la conclusion d'une convention supplémentaire avec les Etats-Unis n'est pas la seule manière de résoudre le problème posé par le fait que le système juridique de l'Union européenne et celui des Etats-Unis ne garantissent pas un niveau équivalent de protection. En outre, une nouvelle convention, même si elle se base sur la Directive 95/46/CE, implique le risque que cette convention soit annulée par la Cour de Justice[3] ou tout au moins qu'il n'y ait pas unanimité au sein du Groupe 29[4] quant à l'équivalence du niveau de protection offert par un tel accord.

Après examen complémentaire, la Commission attire l'attention, dans les rubriques B.2 à B.4 incluses, sur quelques actions alternatives que le Gouvernement belge pourrait envisager d'entreprendre, sur le plan national et international.

B.2. Concertation éventuelle avec les Etats-Unis quant à l'application des accords et procédures déjà existants

La Commission juge surtout opportun de veiller à l'application des traités déjà conclus avec les Etats-Unis et des procédures globales existant déjà en matière de lutte contre le terrorisme. Elle regrette de devoir constater que les Etats-Unis n'ont jusqu'à présent pas signé la Convention n° 108 sur la protection des données à caractère personnel.[5] En dépit de cela, les échanges de données à caractère personnel doivent être effectués dans le respect des principes protecteurs et des garanties applicables en droit européen en ce qui concerne l'échange de données à caractère personnel avec un pays tiers. Les recommandations et procédures suivantes sont déjà applicables :

- Respect des recommandations de la Financial Action Task Force ("FATF") ou Groupe d'Action Financière ("GAFI").[6]
- Echange d'informations financières via les cellules nationales de renseignements financiers ("Financial Intelligence Units" ou "FIUs") opérationnelles dans le cadre du "Groupe Egmont".[7] Concrètement, une procédure a été mise en place pour l'échange d'informations entre le FinCEN (Etats-Unis), la cellule belge dite "Cellule de Traitement des Informations Financières" ou "CTIF" (en néerlandais, "Cel voor Financiële Informatieverwerking" ou "CIF") et les autres cellules de renseignements financiers.

Bien que les procédures susmentionnées s'adressent avant tout aux institutions financières, la question se pose de savoir pourquoi SWIFT devrait être exclue du champ d'application de ces recommandations et procédures. Certes, à l'heure actuelle, SWIFT

[2] Point 6.3. de l'avis n° 10/2006 relatif au traitement par SWIFT de données à caractère personnel cité dans le préambule.
[3] Voir l'arrêt "PNR" de la Cour de Justice, affaires C-317/04 et C-318/04.
[4] Voir les avis du Groupe 29 sur les accords PNR.
[5] Convention du 28 janvier 1981 *pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel* approuvée par la loi du 17 juin 1991 *portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981* (M.B, 30 décembre 1993).
[6] Publiées sur site http://www.fatf-gafi.org Pour ce qui est des 40 recommandations, voir http://www.fatf-gafi.or/dataoecd/42/43/33628117.PDF
[7] Cf. http://www.egmontgroup.org/about_egmont.pdf

n'est pas considérée comme une institution financière par le GAFI.[8] Toutefois, vu que les demandes de transmission d'informations dans le cadre de la lutte contre le terrorisme sont adressées directement à SWIFT, on peut se demander s'il ne serait pas recommandé d'étendre les recommandations existantes à ce type de sociétés qui devraient par conséquent faire rapport aux cellules nationales de renseignements financiers (FIU's).

Par ailleurs, une proposition de décision-cadre du Conseil est également en cours d'élaboration et son champ d'application pourrait être élargi aux transferts opérés par des entreprises européennes à destination d'autorités étrangères[9] (voir infra, rubrique E).

B.3. Actions possibles dans le domaine de la réglementation belge : adaptation de l'article 22, dernier alinéa[10] de la Loi vie privée

Sur le plan des transferts internationaux à des fins privées, le Gouvernement belge pourrait préciser l'actuel article 22 de la Loi vie privée. Pour éviter tout malentendu, par "finalités privées", il n'est pas fait référence aux transferts ultérieurs de données à des autorités publiques ("onward transfers"), comme le transfert de données par SWIFT à l'UST. Afin de faire garantir un niveau de protection équivalent sur ce plan, des solutions doivent être recherchées via des techniques telles qu'une convention entre les Etats-Unis et l'Union européenne[11] ou l'application ou l'amendement de procédures ou de traités existants avec les Etats-Unis.

En outre, conformément aux dernières évolutions du droit européen, les grandes entreprises et multinationales établies en Belgique devraient pouvoir disposer des instruments reconnus sur le plan européen pour régulariser leurs transferts commerciaux internationaux de données à caractère personnel qui relèvent de leurs activités normales sur la base des dispositions relatives aux exceptions de l'article 22 de la Loi vie privée. A cet égard, il existe déjà quelques précédents clairs au niveau des traitements ayant pour but l'administration du personnel et la gestion de la clientèle par des entreprises financières et pharmaceutiques. Une récente conférence internationale organisée par la Commission européenne[12] a montré qu'il existait un consensus croissant concernant l'option, pour les multinationales, de choisir des instruments internationaux tels que les règles d'entreprise contraignantes ("binding corporate rules") ou les clauses contractuelles types adoptées par la Commission européenne ("standard contractual clauses"), conformément à l'article 26, 2 de la Directive 95/46/CE[13], par exemple dans l'hypothèse où d'autres instruments tels que les Principes de sphère de sécurité ("Safe Harbour") ne peuvent pas être appliqués. Le Groupe 29 a rappelé, à juste titre, dans son avis SWIFT, que les règles d'entreprise contraignantes et les clauses contractuelles types[14] sont des solutions envisageables.

Si la Commission a recommandé la solution des règles d'entreprise contraignantes dans son avis SWIFT[15], la faisabilité concrète de cette option en vertu du droit belge mérite

[8] Swift a en effet soutenu devant le GAFI qu'elle n'était qu'une entreprise de télécommunication assurant le transport d'informations et qu'elle ne devait par conséquent pas être soumise à la recommandation n° 7 du GAFI.
[9] Proposition de décision-cadre du Conseil *relative à la protection des données à caractère personnel traitée dans le cadre de la coopération policière et judiciaire en matière pénale* {SEC (2005) 1241}. Voir http://ec.europa.eu/prelex/detail_real.cfm?CL=fr&DosId=193371
[10] Art. 22, dernier alinéa : "*le Roi peut, après avis de la Commission de la protection de la vie privée, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un pays non membre de la Communauté européenne et n'assurant pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privee et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées*".
[11] Voir rubrique E.2.7. de l'avis 37/2006.
[12] Organisée à Bruxelles par la Commission européenne, le Groupe 29 et l'US Department of Commerce les 23 et 24 octobre 2006, programme publié sur http://ec.europa.eu/justice_home/news/events/conference_data_protection/programme_en.pdf
[13] Voir à cet égard : http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_fr.htm
[14] Voir point 4.6.2. de l'avis cité du Groupe 29.
[15] Avis n° 37/2006 de la Commission de la protection de la vie privée du 27 septembre 2006.

également une attention particulière dans le dossier SWIFT et pour d'autres grandes entreprises ou sociétés établies en Belgique. Bien que l'article 22 de la Loi vie privée belge prévoie déjà une procédure d'autorisation via un arrêté royal, la Commission constate qu'il n'y a pas encore de précédent couronné de succès en Belgique dans le cadre duquel la procédure d'autorisation via un arrêté royal a pu aboutir[16]. Cette procédure est peut-être encore trop peu connue ou est-elle confrontée, par ailleurs, à des exigences de formalités et à des discussions juridiques inutiles. Ainsi, on peut se demander si, en vertu du droit belge, un arrêté royal peut reconnaître des règles d'entreprise contraignantes. Vu le consensus européen susmentionné dans l'avis du Groupe 29 et la sécurité juridique requise, la Commission recommande au Gouvernement d'adapter l'article 22, dernier alinéa de la Loi vie privée. De cette manière, les clauses contractuelles types adoptées par la Commission européenne pourraient être explicitement reprises en tant qu'exception, tout comme la référence à des principes de sphère de sécurité admis. Des systèmes tels que les règles d'entreprise contraignantes ("binding corporate rules") devraient pouvoir être acceptés en tant qu'exception, après une autorisation préalable de la Commission de la protection de la vie privée, et cette exception pourrait être reprise explicitement dans la Loi vie privée.

B.4. Absence d'un contrôle efficace de SWIFT en vertu de la réglementation existante visant à prévenir l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme

Sur la base de la Loi vie privée ainsi que des avis SOX et SWIFT du Groupe 29[17], la lutte contre le terrorisme constitue en premier lieu une finalité dans le cadre de laquelle le rôle de SWIFT et la base juridique doivent en principe être examinés par les services compétents, à la lumière de l'ordre juridique européen et de l'ordre juridique belge, conformément aux principes européens de protection des données (article 5 de la Loi vie privée).

Toutefois, la Commission constate qu'actuellement, SWIFT ne tombe pas dans le champ d'application des mécanismes de contrôle et des obligations de rapport existant en Belgique, tels qu'instaurés par la loi du 11 janvier 1993 *relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme*. Seuls les clients de SWIFT, donc des institutions financières, semblent être soumis à cette loi, bien que ceux-ci ne disposent pas des mêmes informations telles que par exemple, les modalités concrètes des transferts à l'UST. Dans cette optique, on peut remettre en cause l'efficacité de la base légale actuelle pour le contrôle de SWIFT. D'éventuelles adaptations apportées à cette base doivent être élaborées conformément aux principes européens (voir rubrique D).

La Commission recommande au Gouvernement d'évaluer s'il faut remédier à cette lacune existante.

Dans ce cadre, il est étonnant que SWIFT affirme constamment que, grâce aux informations qu'elle transmet à l'UST et à la lutte contre le terrorisme, des milliers de vies humaines ont été épargnées.

La Commission fait remarquer que cette affirmation est tout à fait impossible à contrôler, vu qu'aucune vérification précise ne peut être effectuée quant aux résultats.

L'argument de la pertinence des informations fournies par SWIFT dans le cadre de la lutte contre le terrorisme constitue toutefois aussi une arme à double tranchant qui ne soulève pas uniquement la question de savoir si ces informations peuvent ou doivent seulement être mises à la disposition de l'UST. Si ces informations sont absolument nécessaires pour

[16] Cf. le précédent du dossier General Electric, malgré l'avis positif n° 04/2006 du 15 mars 2004.
[17] Voir point 4.2.2. de l'avis Swift du Groupe 29.

la lutte contre le terrorisme, la question se pose de savoir pourquoi ces informations n'ont pas également été communiquées aux services d'ordre et de renseignements européens.

La Commission précise d'ailleurs qu'entre-temps, le principe de réciprocité en matière d'échange d'informations entre les cellules nationales de renseignements financiers belge et américaine a bien été confirmé via l'article 17 de la loi du 11 janvier 1993 (entre la CTIF/CFI et le FinCEN) et un Memorandum of Understanding de 1994 (entre le FinCEN américain et la CTIF/CFI belge).

C. CONTEXTE EUROPEEN

A la suite de l'avis SWIFT, la Commission a reçu, le 8 novembre 2006, une opinion juridique de SWIFT dans laquelle elle contestait l'applicabilité de la Directive 95/46/CE[18], sur la base de l'article 3.2. de la Directive 95/46/CE, et dans laquelle SWIFT faisait référence à la distinction établie entre les trois piliers de l'Union européenne.

Etant donné que cette critique a des implications directes sur l'objet du présent avis (dans l'hypothèse où un accord serait approuvé entre les autorités européennes et les Etats-Unis), la Commission estime nécessaire de rappeler les trois piliers de l'Union européenne. La Commission souhaite ainsi expliquer pour quelles raisons SWIFT part, à tort, du principe que l'UST serait le seul responsable du transfert de données à caractère personnel (au lieu de SWIFT), et pour quelles raisons les principes de la Directive 95/46/CE – tels que mis en œuvre dans la loi belge relative à la vie privée – doivent bel et bien être jugés applicables au transfert par SWIFT de données à caractère personnel à l'UST.

C.1. Trois piliers de l'Union européenne

L'idée selon laquelle l'Union européenne repose sur trois piliers a été lancée en avril 1991 sous la présidence luxembourgeoise via le "non-paper"[19]. Ces trois piliers sont [20] :

1. les dispositions relatives aux communautés ;
2. les dispositions relatives à une politique étrangère et de sécurité commune et
3. les dispositions relatives à la collaboration sur le plan de la Justice et des affaires intérieures.

C.2. Responsabilité de SWIFT

Aux pages 9 à 13 de son avis SWIFT, la Commission motivait déjà en détail pour quelles raisons SWIFT est, selon elle, responsable du transfert commercial normal de données à caractère personnel via le service SWIFTNet FIN et via les transferts à l'UST. La Commission insiste surtout sur les activités concrètes de SWIFT qui, en tant qu'acteur privé, la SCRL SWIFT, tombent dans le champ d'application du premier pilier et donc de la Directive 95/46/CE. La Commission constate qu'entre-temps, les autorités européennes de protection des données se sont rangées à son avis, par un avis uniforme et cohérent formulé par le Groupe 29[21]. A cet égard, il est clairement établi que SWIFT ne peut ignorer sa responsabilité à la lumière de la loi belge relative à la vie privée et de la Directive 95/46/CE.

[18] Voir les pages 11 (points 10 et 11) et 13 de l'opinion de SWIFT.
[19] Europe, doc. n° 1709/1710, 3 mai 1991.
[20] LENAERTS, K. et VAN NUFFEL, P., Europees Recht in hoofdlijnen, Maklu, 2003, page 80 (point 51).
[21] WP128 ou Avis n° 10/2006 *sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, tel que publié sur http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf

C.3. Applicabilité de la Directive 95/46/CE

Vu l'article 3.2. de la Directive 95/46/CE[22], il y a lieu de se demander si SWIFT peut invoquer cet article et si une éventuelle convention d'une autorité belge ou européenne avec les Etats-Unis sur le transfert de données à caractère personnel à l'UST tombe nécessairement dans le champ d'application de la Directive 95/46/CE. Pour éviter tout malentendu, la Commission souligne toutefois que la différence entre le premier et le deuxième pilier n'est pertinente que pour d'éventuelles actions de l'autorité belge ou européenne (voir ci-après au point D.1.). SWIFT elle-même ne peut pas bénéficier d'une disposition d'exception en vertu de la Directive puisqu'elle est soumise à la loi belge relative à la vie privée belge et que cette loi ne fait pas la moindre distinction entre un premier et un troisième pilier.

Dans les arrêts **"Osterreichischer Rundfunk** et autres**"** du 20 mai 2003[23], **Lindqvist** du 6 novembre 2003[24] et **PNR** du 30 mai 2006[25], la Cour de Justice a commenté à plusieurs reprises l'applicabilité de la Directive 95/46/CE. Sur la base des différents éléments pertinents de ces arrêts, nous pouvons avancer ces quelques principes :

- La Directive 95/46/CE a été définie sur la base de l'article 100 A du Traité instituant la Communauté européenne et a pour but de réaliser le marché intérieur qui comprend également la protection du droit à la vie privée. L'effet d'harmonisation de la directive dans ce domaine permet à SWIFT d'éviter des obstacles sur le marché interne et SWIFT jouit, au sein de l'Union européenne, de la garantie d'un règlement cohérent en matière de protection des données. L'avis du Groupe 29 qui a donné, entre-temps, une interprétation uniforme dans le dossier SWIFT constitue une illustration claire de la présence de cette cohérence. La finalité de la directive est précisément poursuivie si celle-ci est appliquée aux divers traitements qui tombent sous la responsabilité de SWIFT au sein de l'Union européenne, y compris les traitements qui impliquent une transmission internationale de données à caractère personnel.

- L'article 3, alinéa 1 de la Directive 95/46/CE définit le champ d'application de manière très large en ne faisant pas dépendre l'applicabilité des règles de protection de la question de savoir si le traitement est effectivement lié à la libre circulation entre les Etats membres. Dans le considérant n° 43 dans l'affaire Rundfünk, la Cour de Justice a jugé que *"l'applicabilité de la directive 95/46 à des situations qui ne comportent pas de lien direct avec l'exercice des libertés fondamentales de circulation garanties par le traité est confirmée par le libellé de l'article 3, paragraphe 1, de cette directive, qui définit le champ d'application de celle-ci de manière très large, en ne faisant pas dépendre l'application des règles de protection de la question de savoir si le traitement comporte un lien effectif avec la libre circulation entre États membres. La même confirmation est donnée par les exceptions contenues au paragraphe 2 du même article, en particulier celles ayant trait au traitement de données à caractère personnel "mis en œuvre pour l'exercice d'activités [...] prévues aux titres V et VI du traité sur l'Union européenne» ou encore pour "l'exercice d'activités exclusivement personnelles ou domestiques». En effet,*

[22] Qui dispose ce qui suit : *"2. La présente directive ne s'applique pas aux traitements de données à caractère personnel :*
- mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat (y compris le bien-être économique de l'Etat lorsque ces traitements sont liés à des questions de sûreté de l'Etat) et les activités de l'Etat relatives à des domaines du droit pénal; (...)"
[23] Jugement du 20 mai 2003 dans l'affaire C-465/00 (Rechnungshof / Osterreichischer Rundfunk et autres), disponible sur http://www.curia.europa.eu/fr/content/juris/index_form.htm
[24] Affaire C-101/01.
[25] Affaires C-317/04, C-318/04.

ces dérogations ne seraient, à tout le moins, pas libellées de cette manière si ladite directive était exclusivement applicable à des situations comportant un lien suffisant avec l'exercice des libertés de circulation."

- Le transfert de données à caractère personnel par SWIFT à l'UST ne tombe pas dans le champ d'application de l'article 3, alinéa 2 parce qu'il s'agit de traitements et d'activités d'une entreprise privée, la SCRL SWIFT, et pas de traitements ou d'activités d'un Etat membre[26]. Dans son analyse juridique susmentionnée, SWIFT atténue, à tort, sa propre contribution et minimalise clairement son propre rôle. Elle invoque une exception qui n'est prescrite que pour une action effectuée par des autorités européennes au sein du troisième pilier.

- Enfin, le transfert de données à caractère personnel par SWIFT à l'UST ne tombe pas dans le champ d'application de l'article 3, alinéa 2 parce que, contrairement à l'affaire PNR, SWIFT, lors de la communication de données à caractère personnel à l'UST, ne s'est nullement basée sur un cadre ou un accord antérieur avec des instances publiques européennes selon lequel (seule) cette action de l'autorité tomberait en dehors du champ d'application de la directive. Seules les décisions 2004/496/CE du 17 mai 2004 et 2004/535/CE du 14 mai 2004 constituaient des activités concrètes d'un service public dans les domaines nommés à l'article 3, alinéa 2 et seule ces activités tombaient en dehors du champ d'application de la Directive 95/46/CE. Autrement dit, l'affaire PNR ne signifie pas que les compagnies aériennes ne tomberaient pas (ne tomberaient plus) dans le champ d'application de la Directive 95/46/CE pour leurs divers traitements.

D. ELEMENTS DE FOND D'UNE CONVENTION AU NOM DU GOUVERNEMENT BELGE : LA DIRECTIVE 95/46/CE ET L'ARTICLE 8 DE LA CEDH COMME POINT DE DEPART

D.1. Cohérence requise avec les principes de la Directive 95/46/CE

Dans la logique de l'arrêt PNR, une éventuelle convention au nom de la Belgique ou de l'Union européenne avec les Etats-Unis au sujet du domaine pertinent de la lutte contre le terrorisme constitue bien un acte qui pourrait tomber dans le champ d'application de l'article 3, alinéa 2 de la Directive 95/46/CE. En fait, si cette action gouvernementale belge ou européenne peut tomber en dehors du champ d'application de la Directive 95/46/CE, la question se pose en effet de savoir si les principes propres à la Directive 95/46/CE peuvent ou doivent encore être repris dans la convention.

On peut se référer ici au point de vue constant et commun des autorités européennes en matière de protection des données. Il ressort des déclarations que ces autorités ont formulées dans le courant de cette année à Budapest[27] et à Londres[28] que l'échange de données à caractère personnel avec des instances policières et judiciaires ne peut être considéré comme admissible que sur la base de règles de protection des données qui **offrent un niveau de protection élevé, consistant et équivalent à celui du premier pilier**. La Commission se réfère à cet égard au point de vue du Contrôleur européen de la protection des données (CEPD)[29] au sujet de la proposition de décision-cadre du Conseil

[26] Dans le considérant 43 de l'arrêt Lindqvist, il était déjà stipule que : *"Les activités mentionnées à titre d'exemples à l'article 3, paragraphe 2, premier tiret, de la directive 95/46 (à savoir les activités prévues aux titres V et VI du traité sur l'Union européenne ainsi que les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités relatives à des domaines du droit pénal) sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers. »*. Voir également le considérant 58 de l'affaire PNR.

[27] Declaration adopted at the Conference of European Data protection Authorities in Budapest from 24 to 25 April 2006.

[28] Declaration adopted by the European Data Protection Authorities in London on 2 November 2006.

[29] Dans le point 39 de l'avis 2006/C/47, le CEPD mentionne ce qui suit : "*Toutefois, dans l'hypothèse où des données pourraient être transmises à un pays tiers sans que la protection de la personne concernée soit garantie, cela porterait gravement atteinte à la protection envisagée par la proposition considérée sur le territoire de l'Union européenne, pour*

précitée, où l'importance du maintien de règles strictes en matière de protection des données a été soulignée lorsqu'il s'agit de transmettre des données à caractère personnel à des pays tiers. Dans le niveau de protection susmentionné, un certain nombre de garanties essentielles (sans être exhaustif) sont concrètement reprises, telles que les exigences de transparence, de proportionnalité et de nécessité, le droit d'accès et le contrôle indépendant.

D.2. Eléments des accords Safe Harbour et PNR suite à la Directive 95/46/CE

Dans l'accord Safe Harbour et le récent accord (intérimaire) adopté en matière de PNR le 16 octobre 2006[30], on est toujours parti d'un niveau de protection inspiré de la Directive 95/46/CE.

L'équivalence de ces accords à l'égard de la Directive 95/46/CE a cependant été critiquée par le Groupe 29[31]. Le fait que le Groupe 29 n'ait pas émis une appréciation positive unanime sur l'accord PNR et l'affaire PNR du 30 mai 2006[32] devant la Cour de Justice démontre que de tels accords avec les Etats-Unis sont assez délicats.

D.3. Eléments complémentaires de la proposition de décision-cadre du Conseil

Outre la cohérence requise avec les principes de la Directive 95/46/CE, il a été admis que les caractéristiques particulières des objectifs dans le troisième pilier nécessitent de prévoir des principes complémentaires à ceux formulés dans la Directive 95/46/CE.

Dans l'exposé des motifs de la proposition de décision-cadre[33], la Commission européenne a déjà commenté le 4 octobre 2005 les exigences de cohérence avec la Directive 95/46/CE ainsi que les principes de protection complémentaires. Le CEPD a également mentionné au point 9 de son avis portant sur la proposition de décision-cadre que : "*Ce nouveau cadre devrait non seulement respecter les principes de la protection des données énoncés dans la directive 95/46/ CE - il importe de garantir la cohérence de la protection des données au*

---

les raisons évoquées dans la partie III.4 ci-dessous. En résumé : - Il serait directement porté atteinte aux droits de la personne concernée, tels qu'ils sont garantis par la proposition considérée, si la transmission aux pays tiers n'était pas soumise aux règles régissant la protection des données ; - il existerait un risque que les autorités compétentes des Etats membres contournent les normes strictes applicables à la protection des données."

[30] Adopté à la suite de l'arrêt PNR de la Cour de Justice, qui stipule : "*Le présent accord n'a pas pour objet de déroger à la législation des Etats-Unis d'Amérique ou de l'Union européenne ni de la modifier ; il ne crée ni ne confère aucun droit ou avantage sur toute autre personne ou entité, privée ou publique*". Voir la Décision 2006/729/PESC/JAI du Conseil du 16 octobre 2006 *relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données contenues dans les dossiers des passagers (données PNR) par des transporteurs aériens au ministère américain de la sécurité intérieure - Accord entre l'Union européenne et les Etats-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure*, Journal officiel N° L 298 du 27/10/2006, pp. 0027 – 0031.

[31] Voir les avis du Groupe 29 au sujet de ces accords.

[32] Affaires C-317/04, C-318/04

[33] Voir l'exposé des motifs (page 6) de la proposition de décision-cadre : "*Il convient de reconnaître les particularités du traitement et de la protection des données dans le cadre du titre VI du traité sur l'Union européenne. D'une part, ces spécificités ne doivent pas faire obstacle à la cohérence avec la politique générale de l'Union dans le domaine du respect de la vie privée et de la protection des données sur le fondement de la Charte des droits fondamentaux et de la directive 95/46/CE. Les principes fondamentaux de la protection des données s'appliquent au traitement des données dans le cadre des premier et troisième piliers. D'autre part, la cohérence doit être assurée avec les autres instruments qui prévoient des obligations spécifiques en ce qui concerne les informations susceptibles d'être pertinentes aux fins de la prévention et de la lutte contre la criminalité. Il convient de suivre l'évolution de la situation en ce qui concerne la conservation des données traitées et stockées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou des données transmises sur les réseaux de télécommunications publics aux fins de prévention et de détection des infractions pénales, y compris du terrorisme, et d'enquêtes et de poursuites en la matière. Il convient tout particulièrement de prendre en considération le rapport étroit qui existe entre le présente proposition de décision-cadre et la proposition de la Commission visant à adopter une directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE.*"

sein de l'Union européenne -, mais aussi prévoir un ensemble complémentaire de règles tenant compte de la nature spécifique du domaine répressif".

D.4. Eléments de l'article 8 de la CEDH

La Commission rappelle également la jurisprudence détaillée de la Cour Européenne des Droits de l'Homme dans ce domaine, sur la base de l'article 8 de la CEDH qui fournit des éléments de fond pour une éventuelle convention avec les Etats-Unis. On peut notamment, et de nouveau sans être exhaustif, se référer aux exigences de nécessité d'ingérence dans une société démocratique et à l'exigence de transparence de la norme en vertu de l'article 8 de la CEDH.

E. FORME DE LA CONVENTION VISEE PAR LE GOUVERNEMENT

Une éventuelle convention avec les Etats-Unis concernant la communication de données à caractère personnel à l'UST risque de ne pas tomber dans le champ d'application de la Directive 95/46/CE, dès lors que la convention visée par le Gouvernement belge relèverait du troisième pilier.

Il existe actuellement dans le troisième pilier différentes actions et discussions européennes telles que, en particulier, la proposition de décision-cadre qui est négociée en ce moment dans le troisième pilier.

La proposition de décision-cadre est une initiative qui se situe dans le troisième pilier[34] et qui porte sur la protection de données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale. Bien que cette proposition ne règle pas (encore) spécifiquement au sens strict la problématique du transfert de données à caractère personnel par des entreprises européennes à des autorités publiques extérieures à l'Union européenne, des propositions d'élargissement de la proposition ont été proposées. La Commission se réfère à l'avis[35] du contrôleur européen de la protection des données ("CEPD") du 19 décembre 2005 et au Rapport du 18 mai 2006 relatif à la proposition, dont le rapporteur est madame Martine Roure[36]. L'avis et la proposition précités visent précisément à étendre le champ d'application de la décision-cadre du Conseil aux transferts d'entreprises européennes privées à des autorités publiques européennes et aux transferts d'autorités publiques européennes à des autorités publiques non européennes.

Bien qu'il n'existe encore actuellement aucune position ou proposition formelle pour réglementer les transferts d'entreprises européennes privées à des autorités publiques non européennes, tels que ceux de SWIFT à l'UST, il est possible que le Gouvernement belge ou un autre Etat membre inscrive cette discussion à l'ordre du jour européen, suite aux propositions d'amendements antérieures. Cette action pourrait viser l'élaboration d'une solution équilibrée et uniforme dans le troisième pilier, en présentant un niveau de protection adéquat et équivalent à celui de la Directive 95/46/CE.

---

[34] Proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale {SEC(2005)1241}. Voir http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=fr&DosId=193371

[35] Avis du contrôleur européen de la protection des données sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM (2005) 475 final), publié sur le site Internet http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2006/c_047/c_04720060225fr00270047.pdf

[36] Rapport du 18 mai 2006 sur la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, A6-192/2006, PE 370.250/v02-00.

Etant donné l'implication belge spécifique, en raison du fait que la responsabilité d'une société belge est engagée, la diplomatie belge pourrait en outre également intervenir auprès de l'autorité américaine afin que soient explicitées l'utilisation et les modalités des traitements effectués aux Etats-Unis.

PAR CES MOTIFS,

Sur la base de son examen général et sans préjudice de la compétence des institutions et des contrôleurs européens tels que le CEPD de prendre ultérieurement une position à cet égard, la Commission estime que :

- En ce qui concerne les traitements commerciaux de données à caractère personnel par SWIFT, la loi belge relative à la vie privée et la Directive 95/46/CE restent, comme mentionné précédemment, intégralement d'application et SWIFT se doit de respecter la Loi vie privée.
- En ce qui concerne la conclusion d'une convention spécifique avec les Etats-Unis, la Commission considère qu'il ne s'agit pas du seul moyen pour résoudre l'absence d'un niveau de protection équivalent entre les systèmes juridiques de l'Union européenne et des Etats-Unis.
- L'on pourrait également tenter au préalable d'adapter les accords déjà conclus et les procédures existantes en matière de lutte contre le terrorisme conformément aux principes européens de protection en vigueur, aux recommandations du GAFI et aux procédures d'échange de données à caractère personnel via les cellules nationales de renseignements financiers.
- Le champ d'application de la proposition de décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (SEC-2005-1241) pourrait être amendé de sorte que des transferts de données privées tels que ceux de SWIFT à des instances publiques comme l'UST soient réglementées plus clairement au niveau européen.
- Pour les transferts internationaux réalisés à des fins privées, le Gouvernement belge pourrait préciser l'actuel article 22 de la Loi vie privée, conformément au consensus européen existant.

La Commission constate ensuite que SWIFT ne relève actuellement pas du champ d'application des mécanismes de contrôle financier et des obligations de rapport existant en Belgique et de manière globale, tels que la loi du 11 janvier 1993 et les recommandations du GAFI. Etant donné que les demandes de transmission d'informations ont été adressées directement à SWIFT dans le cadre de la lutte contre le terrorisme, la Commission recommande au Gouvernement d'apprécier si cette lacune est souhaitée et s'il convient d'y remédier et dans quelle mesure, conformément aux principes de protection européens applicables.

La Commission se tient également à la disposition du Gouvernement belge s'il fallait éventuellement collaborer avec les autorités américaines compétentes en vue de mener une enquête visant à apporter des éclaircissements quant à l'utilisation qui a été faite des données transmises. La Commission de la protection de la vie privée espère que cette enquête concrète pourra se faire. Elle vérifie dans quelle mesure elle peut analyser cela, en collaboration avec les autorités compétentes, en particulier les DPA (data protection authority's).

Subsidiairement, compte tenu de la critique antérieure du Groupe 29 quant au niveau de protection des accords Safe Harbour et PNR, la Commission souligne que la convention envisagée par le Gouvernement doit quoi qu'il en soit assurer, au niveau de son contenu, un niveau de protection élevé, conformément au niveau de protection européen déjà offert par la Directive 95/46/CE et la Convention n° 108[37].

Vu la matière complexe et son importance, la Commission se tient à disposition pour émettre des avis ultérieurs concernant cette problématique.

L'administrateur, Le vice-président,

(sé) Jo BARET (sé) Willem DEBEUCKELAERE

[37] Convention du 28 janvier 1981 *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, M.B., 30 décembre 1993, approuvée par la loi du 17 juin 1991 *portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981.*