//COMMISSION DES AFFAIRES EUROPÉENNES//

##Mercredi 28 octobre 2009## - <u>Présidence de M. Hubert Haenel</u> -

@@Justice et affaires intérieures@@

&&Accord entre l'Union européenne et les États-Unis sur le transfert de données de messagerie financière (Accord « Swift »)

*Communication de M. Hubert Haenel***&&**

M. Hubert Haenel. – Nous devons examiner aujourd'hui le **projet d'accord** entre l'Union européenne et les États-Unis sur le transfert de données détenues par la société SWIFT. La semaine dernière, nous avons entendu notre collègue Alex Türk, président des « CNIL européennes » qui est venu nous parler de cette affaire. A cette occasion, je vous avais fait part de l'échange de lettres que j'ai eu cet été avec le Gouvernement. J'avais demandé un report de l'adoption du texte qui permettait l'ouverture des négociations. Aujourd'hui, nous sommes saisis du texte même du projet d'accord qui a été négocié.

Je dois signaler qu'**il ne s'agit pas d'un texte définitif.** Il est précisé dans ce projet d'accord que *« les délégations de l'UE et des États-Unis ne sont encore parvenues à un consensus définitif sur aucun des volets de ce projet d'accord. Les deux parties doivent mener des consultations en interne sur le projet de texte en prévision de la prochaine série de négociations. »* Le document transmis le 9 octobre, qui relatait le dernier état de la négociation, est donc un texte susceptible de recevoir des modifications, voire des changements substantiels.

La Présidence prévoit une adoption probable lors du Conseil JAI des 30 novembre et 1er décembre 2009. En nous prononçant aujourd'hui, nous sommes

donc en mesure de faire valoir utilement notre point de vue et de le faire connaître au Gouvernement.

I - QUEL EST L'HISTORIQUE DE CE DOSSIER ?

SWIFT, société coopérative de droit belge, est un prestataire international de services informatiques qui facilite les opérations financières grâce à un réseau de communication et un système de messagerie standardisée. Plus de 8 000 organisations bancaires, institutions financières et leurs clients professionnels échangent par ce biais, 15 millions de messages par jour dans de nombreux domaines d'activité du secteur bancaire et des titres, notamment celui des paiements de masse *(virements, paiements par cartes de crédit).*

SWIFT transporte des messages standardisés entre deux établissements financiers sans traiter autrement ni stocker de façon prolongée les messages qu'il véhicule. L'architecture du système SWIFT repose actuellement sur un centre d'exploitation mondial situé aux Pays-Bas. La sauvegarde des informations traitées est assurée par la duplication de la base de données néerlandaise dans une base de données située aux États-Unis (*en Virginie*).

Après les attentats du 11 septembre 2001, le département du Trésor des États-Unis a mis au point un programme de surveillance du financement du terrorisme. Dans ce cadre, il est apparu, en 2006, que des injonctions administratives avaient été adressées à la société SWIFT pour que les bureaux de cette entreprise implantés aux États-Unis transfèrent au bureau du contrôle des avoirs étrangers des données à caractère personnel devant servir à agir contre les personnes soupçonnées d'activités terroristes.

En novembre 2006, le groupe dit « de l'article 29 » (qui réunit les « CNIL » européennes) a émis un avis selon lequel SWIFT et les institutions financières utilisant ses services violaient la législation communautaire en matière de protection des données, notamment en n'assurant pas une protection adéquate dans le cadre du transfert de données vers les États-Unis et en n'informant pas les personnes concernées du traitement des informations les concernant.

Des négociations engagées en décembre 2006 sous l'égide de la Commission européenne avec le département du Trésor américain ont abouti à des engagements unilatéraux américains *(sous la forme d'un échange de lettres, publiées au Journal officiel de l'Union européenne en juillet 2007).* Destinés à répondre aux préoccupations européennes sur la protection des données, ces engagements comportaient quatre éléments principaux : l'utilisation des données pour des finalités de lutte contre le terrorisme, à l'exclusion de toute autre finalité notamment commerciale ou industrielle (*cette limitation étant étendue aux agences américaines et aux États tiers avec lesquels les données seraient partagées*) ; un effort d'identification et d'effacement « au fil de l'eau » des données transmises qui n'apparaîtraient pas nécessaires aux investigations du contre-terrorisme ; la conservation des données sur une base dormante pour une durée maximale de cinq ans ; la désignation d'une « éminente personnalité » européenne chargée d'évaluer le respect des engagements américains.

En mars 2008, l'Union européenne a désigné M. Jean-Louis Bruguière pour cette fonction, pour une durée de deux ans et avec pour mission de présenter un rapport annuel. Dans un rapport rendu au début de l'année à l'issue de trois missions à Washington, M. Bruguière a estimé que le Trésor américain s'était mis correctement à sa disposition et qu'il avait apporté la démonstration du respect des

garanties prévues. Les autorités américaines auraient donc respecté leurs engagements sur la protection des données provenant de l'Union européenne ; l'exploitation de ces données aurait permis d'accroître l'efficacité de la lutte contre le terrorisme et son financement. Le rapport formule certaines recommandations techniques et déplore le fait que la législation américaine réserve le droit au recours judiciaire aux citoyens et résidents permanents des États-Unis. Il suggère d'étendre le dispositif à la lutte contre le crime organisé et recommande de réexaminer le cadre juridique de l'accord, compte tenu de la nouvelle architecture informatique de SWIFT. Cependant, ce rapport a été classifié secret à la demande des autorités américaines car il comporterait certaines informations sur les modes opératoires du contre-terrorisme américain. Il n'était donc pas possible d'en avoir une connaissance exhaustive. Notre collègue Alex Türk nous a indiqué, la semaine dernière, qu'à la suite de demandes réitérées de sa part, M. Bruguière lui en avait transmis une synthèse et que l'intégralité du rapport serait désormais consultable par des personnes habilitées.

II - EN QUOI LA NOUVELLE « ARCHITECTURE » DE SWIFT JUSTIFIE-T-ELLE LA NÉGOCIATION D'UN NOUVEL ACCORD ?

Décidée en octobre 2007, la nouvelle organisation de SWIFT, selon un modèle dit d'« architecture distribuée », distinguera deux zones de traitement : la zone européenne et la zone transatlantique. En conséquence, les messages internes à l'espace européen seront traités et stockés exclusivement dans deux centres européens *(aux Pays-Bas et en Suisse)*. Les messages internes aux États-Unis seront traités aux États-Unis avec une sauvegarde en Suisse. Concrètement, cela signifie qu'une part importante des données qui font l'objet des injonctions administratives dans le cadre du programme du département du Trésor américain ne sera plus

stockée aux États-Unis. Cette réorganisation, qui représente un coût de 150 millions d'euros, répond à la volonté de SWIFT de dissiper les craintes européennes sur la protection des données et de surmonter l'insécurité juridique résultant du conflit entre les normes européennes et américaines en vigueur.

Devant être opérationnelle à la fin 2009, la nouvelle architecture priverait les autorités américaines de l'accès à une partie importante des informations exploitées par le département du Trésor. Or le programme de surveillance du financement du terrorisme s'étant révélé utile pour les États membres, la Commission européenne a proposé l'ouverture de négociations avec les États-Unis en vue de conclure un nouvel accord qui assure la continuité du dispositif indépendamment de la nouvelle architecture de SWIFT.

Le 29 juillet 2009, le Conseil a donc adopté un mandat dans ce sens à la présidence. Des négociations avec la délégation américaine ont eu lieu en septembre. Elles ont permis d'élaborer un projet d'accord en date du 28 septembre qui a été transmis à la commission des affaires européennes le 9 octobre 2009.

III - QUE DIT, EN L'ÉTAT, LE PROJET D'ACCORD ?

En l'état, ce projet d'accord qui ne concernerait que les données SWIFT, prévoit leur transmission exclusivement aux fins de la lutte contre le terrorisme *(article premier)*. Il donne une définition du terrorisme qui ne correspond pas aux définitions européennes ni au mandat de négociation et qui s'apparente à la définition américaine *(article 2)*. Il détaille la procédure de demande et de transmission des données *(article 4)* : la demande devra recenser aussi clairement que possible les données en cause, justifier la nécessité de l'obtention des données ; l'État requis vérifiera la conformité de la demande avec l'accord bilatéral conclu en matière

d'entraide judiciaire ; le fournisseur des données (SWIFT) devra tenir un registre détaillé des données transmises ; le Trésor américain devra effacer des données transmises alors qu'elles ne faisaient pas partie de la demande. Une réciprocité dans la transmission des données est prévue, notamment au profit d'Europol et d'Eurojust *(article 7 et 8)*.

L'accord prévoit par ailleurs des dispositions sur la protection des données *(article 5)* : outre la finalité exclusive, il précise que les garanties dans ce domaine devront être appliquées sans discrimination, notamment sur la base de la nationalité ou du pays de résidence ; les recherches sur ces données devront s'appuyer sur des éléments de preuve préexistants ; les données devront être conservées dans un environnement sécurisé et stockées de manière séparée ; l'accès sera limité aux analystes enquêtant sur le terrorisme et les données ne pourront être partagées qu'avec des services répressifs pour la finalité de lutte contre le terrorisme ; les données qui ne sont plus nécessaires devront être effacées ; un délai maximum de conservation de cinq ans est par ailleurs prévu *(sauf si une enquête se poursuit)*. Toute personne pourra demander à l'autorité chargée de la protection des données dans l'État membre dans lequel le fournisseur est établi la confirmation que ses droits en matière de protection des données ont été respectés et qu'aucun traitement la concernant n'a été fait en violation de l'accord. Un droit de recours administratif ou juridictionnel effectif devra lui être ouvert (*article 12*). En outre, un « droit d'alerte » est reconnu aux autorités chargées de la protection des données, qui provoquera une consultation entre les parties à l'accord pour trouver une solution qui satisfasse cette autorité (*article 13 bis*).

Un réexamen conjoint de l'accord sera réalisé après un délai de six mois (*article 11*). Sauf décision contraire des parties, l'accord prendra fin à l'expiration

d'un délai de douze mois à compter de la date de sa signature. Il aura en effet un caractère intérimaire. A compter de la date de l'entrée en vigueur du traité de Lisbonne, de nouvelles négociations seraient engagées pour conclure un nouvel accord international dans le cadre juridique et institutionnel issu du traité.

IV - QUELLES SONT LES DIFFICULTÉS POSÉES PAR CE PROJET D'ACCORD QUI APPELLENT UNE PARTICULIÈRE VIGILANCE ?

On nous assure que cet échange d'informations a produit des résultats efficaces dans la lutte contre le terrorisme. C'est évidemment un enjeu essentiel et je crois que nous ne pouvons que prendre acte du constat effectué tant par la Commission européenne, le Conseil et la personnalité éminente européenne. Mais nous devons demander qu'à l'avenir l'accès aux évaluations soit plus largement permis, afin de pouvoir vérifier la réalité de ce constat.

La Commission européenne fait par ailleurs valoir la grande convergence entre le mandat donné par le Conseil et le projet d'accord. Si, en l'état, celui-ci prévoit un certain nombre de garanties, il conviendra de s'assurer que ces garanties demeureront dans l'accord final et que certaines incertitudes seront levées. Je crois que nous pouvons identifier plusieurs enjeux sur lesquels je vous proposerai de marquer notre particulière vigilance dans une proposition de résolution :

a) La finalité de la transmission des données

Le projet d'accord mentionne expressément la lutte contre le terrorisme comme finalité exclusive de la transmission de données. Nous devons demander expressément à ce que cette finalité exclusive soit bien retenue dans l'accord final.

Nous devons également demander que soit examinée la compatibilité de la définition du terrorisme qui figurera dans l'accord avec la définition européenne, telle qu'elle résulte de la décision-cadre du 13 juin 2002.

b) la définition et le rôle des autorités compétentes pour la transmission des données

La qualité et les missions qu'aura l'autorité européenne responsable de la transmission des données constituent un autre enjeu crucial. Comme l'a souligné notre collègue Alex Türk, il est indispensable que cette autorité puisse exercer un contrôle effectif sur la conformité des demandes aux conditions posées par le projet d'accord et par l'accord bilatéral sur l'entraide judiciaire.

c) Le partage de l'information

Nous entendons limiter la finalité de la transmission des données à la lutte contre le terrorisme. Nous devons aussi veiller à ce que des garanties soient données sur la conservation des données et que l'accès aux données soient réservées à des services dûment habilités et pour cette seule finalité. La communication des données à des tiers doit être prohibée.

d) Le délai de conservation des données

Une définition rigoureuse du délai de conservation des données doit être prévue. Je rappelle que, pour le PNR européen, le Sénat a proposé une durée de 3 ans, qui pourrait être complétée par un nouveau délai de 3 ans pour les données ayant montré un intérêt particulier. Sans nous prononcer sur un délai précis qui demanderait une expertise plus approfondie, je crois que nous devons demander que

le délai de conservation soit proportionné aux finalités de l'accord et que celui-ci détermine un délai raisonnable.

e) Le droit des personnes concernées

La mise en place d'un droit effectif, pour les personnes concernées, à un recours administratif et judiciaire est un autre enjeu. Ce droit doit pouvoir s'exercer dans un État membre de l'Union européenne comme aux États-Unis. Or la législation américaine, qui, en l'état, ne sera pas affectée par l'accord, réserve le droit au recours judiciaire aux citoyens et résidents permanents des États-Unis. Il y a là un vrai motif de préoccupation.

f) le rôle des autorités de contrôle de la protection des données dans la supervision et l'évaluation de l'accord

Les autorités de contrôle de la protection des données doivent jouer un rôle effectif pour superviser et évaluer la mise en œuvre de l'accord. Il me paraît notamment important que le groupe des « CNIL européennes » que préside notre collègue Alex Türk soit étroitement associé à ces procédures.

Notre collègue nous a aussi fait part du secret qui a entouré le rapport d'évaluation de M. Bruguière. Nous devons demander que les résultats de la supervision et de l'évaluation de l'accord soient accessibles, en particulier au bénéfice des parlements nationaux.

g) La reconduction de l'accord

Enfin, cet accord doit avoir un caractère simplement provisoire. Dès l'entrée en vigueur du traité de Lisbonne, des négociations devront s'ouvrir en vue de

la conclusion d'un nouvel accord. Les nouvelles bases juridiques permettront, en effet, la pleine participation du Parlement européen et des parlements nationaux.

M. Roland Ries. – C'est un dossier complexe. Mais je crois qu'il est essentiel de prévoir des garanties sur la confidentialité et la protection des données personnelles.

Je m'interroge sur la perspective d'un nouvel accord. Quel sera l'impact de l'entrée en vigueur du traité de Lisbonne ?

M. Hubert Haenel. – Avec le traité de Lisbonne, la procédure de codécision s'appliquera. En conséquence, le Parlement européen participera pleinement à la renégociation de l'accord. En toute hypothèse, à l'expiration d'une période de douze mois, l'accord sera caduc. Il devra donc être renégocié soit sur les bases juridiques actuelles, soit sur les nouvelles bases prévues par le traité de Lisbonne.

M. Richard Yung. – La nouvelle négociation se fera donc sous le contrôle du Parlement européen. Cela me paraît une bonne chose. Mais la tâche des négociateurs risque d'être difficile.

M. Hubert Haenel. – La clause de caducité est essentielle. Elle rend l'accord inapplicable à l'expiration du délai de douze mois. Elle ouvre donc la voie à une nouvelle négociation.

M. Christian Cointat. – Ne pouvait-on attendre l'entrée en vigueur du traité de Lisbonne pour négocier cet accord ?

M. Hubert Haenel. – Aux yeux des Américains, cela n'était pas possible. À partir du moment où SWIFT recourait au centre installé en Suisse, les États-Unis n'auraient plus eu accès aux données. Or, ils estiment que cet échange d'informations est indispensable pour assurer la continuité de la lutte contre le terrorisme.

*

A l'issue de ce débat, la commission a conclu à l'unanimité au dépôt de la proposition de résolution suivante :

Proposition de résolution

Le Sénat,

Vu l'article 88-4 de la Constitution ;

Vu le projet d'accord en date du 28 septembre 2009 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 d'Amérique aux fins du programme de surveillance du financement du terrorisme (Accord « SWIFT ») ;

– prenant acte que ce projet d'accord tend à permettre un échange mutuel d'informations entre l'Union européenne et les États-Unis d'Amérique, afin de prévenir et de combattre le terrorisme et son financement, et qu'il fera l'objet d'une prochaine série de négociations ;

– considère qu'un tel échange mutuel d'informations ne peut se concevoir que sous réserve que soient réunies toutes les garanties de nature à assurer un respect effectif des droits fondamentaux, en particulier le droit au respect de la vie privée et à la protection des données à caractère personnel ;

– souligne que les finalités de la transmission des données doivent être strictement délimitées et concerner la prévention et la détection du terrorisme ou de son financement ainsi que les enquêtes et/ou les poursuites en la matière, à l'exclusion de toute autre finalité ;

– demande que la définition du terrorisme qui est retenue dans le projet d'accord fasse l'objet d'une expertise juridique afin de vérifier sa compatibilité avec celle qui résulte de l'article 1er de la décision-cadre 2002/475/JAI du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme ;

– juge nécessaire que la qualité et les missions de l'autorité responsable de recevoir les demandes du département du Trésor américain soient définies précisément et que cette autorité puisse exercer un contrôle effectif de la conformité des demandes de transmission de données aux conditions fixées par le projet d'accord et par l'accord bilatéral en matière d'entraide judiciaire ;

– considère que des garanties très strictes doivent être prévues pour la conservation des données fournies afin notamment de prévenir tout accès non autorisé, que l'accès aux données doit être exclusivement réservé à des services, organismes ou autorités dûment habilités et pour les seules finalités énoncées dans le projet d'accord et que toute communication de ces données à des tiers doit être prohibée ;

– demande que le délai de conservation des données fournies soit proportionné aux finalités énoncées par le projet d'accord et qu'un délai raisonnable soit déterminé ;

– estime que des garanties doivent être établies sur les droits des personnes concernées, en particulier pour leur permettre d'exercer un recours administratif ou juridictionnel effectif tant dans un État membre de l'Union européenne qu'aux États-Unis ;

– demande que le rôle des autorités indépendantes sur la protection des données soit affirmé clairement pour la supervision et l'évaluation de la mise en œuvre de l'accord et son réexamen, qu'en particulier le groupe de travail institué par l'article 29 de la directive 95/46/CE 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 soit étroitement associé à ces procédures ;

– considère que les parlements nationaux devront avoir accès aux résultats de cette supervision et à l'évaluation qui sera faite de l'accord ;

– souligne, d'une part, que l'accord devra expressément mentionner qu'il s'appliquera à titre provisoire en vertu d'une clause de caducité ne pouvant excéder douze mois et, d'autre part, que, dès l'entrée en vigueur du traité de Lisbonne qui sera notifiée aux autorités américaines, un nouvel accord devra être négocié et conclu sur les nouvelles bases juridiques prévues par le traité.