



PARLEMENT EUROPÉEN

2009 - 2014

Document de séance

A7-0013/2010

5.2.2010

RECOMMANDATION

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 (05305/1/2010REV – C7-0004/2010 – 2009/0190(NLE))

Commission des libertés civiles, de la justice et des affaires intérieures

Rapporteure: Jeanine Hennis-Plasschaert

Légende des signes utilisés

- * Procédure de consultation
- *** Procédure d'approbation
- ***I Procédure législative ordinaire (première lecture)
- ***II Procédure législative ordinaire (deuxième lecture)
- ***III Procédure législative ordinaire (troisième lecture)

(La procédure indiquée est fondée sur la base juridique proposée dans le projet d'acte.)

Amendements

Dans les amendements du Parlement, les modifications souhaitées sont indiquées en ***gras et italique***. Pour les actes modificatifs, les parties reprises telles qu'elles d'une disposition existante que le Parlement souhaite amender, alors que le projet d'acte ne l'a pas modifiée, sont marquées en **gras**. D'éventuelles suppressions concernant de tels passages sont signalées comme suit: [...]. Le marquage en *italique maigre* est une indication à l'intention des services techniques qui concerne des éléments du texte législatif pour lesquels une correction est proposée en vue de l'élaboration du texte final (par exemple, éléments manifestement erronés ou manquants dans une version linguistique). Ces suggestions de correction sont subordonnées à l'accord des services techniques concernés.

SOMMAIRE

	Page
PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN	5
EXPOSÉ DES MOTIFS	6
RÉSULTAT DU VOTE FINAL EN COMMISSION	13

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

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 (05305/1/2010REV – C7-0004/2010 – 2009/0190(NLE))

(Procédure de l'avis conforme)

Le Parlement européen,

- vu la proposition de décision du Conseil (COM(2009)0703 et 5305/1/2010REV),
 - vu le texte 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 (16110/2009),
 - vu sa résolution du 17 septembre 2009 sur l'accord international envisagé pour mettre à la disposition du ministère du Trésor des États-Unis des données de messagerie financière afin de prévenir et de combattre le terrorisme et le financement du terrorisme¹,
 - vu la demande d'avis conforme présentée par le Conseil conformément à l'article 218, paragraphe 6, point a), en liaison avec les articles 82, paragraphe 1, point d) et 87, paragraphe 2, point a) du traité sur le fonctionnement de l'Union européenne (C7-0004/2010),
 - vu l'article 81 et l'article 90, paragraphe 8, de son règlement,
 - vu la recommandation de la commission des libertés civiles, de la justice et des affaires intérieures (A7-0013/2010),
1. refuse son avis conforme sur la conclusion de l'accord;
 2. demande à la Commission de présenter immédiatement des recommandations au Conseil en vue d'un accord à long terme avec les États-Unis sur la prévention du financement du terrorisme; rappelle que tout nouvel accord dans ce domaine devra respecter le nouveau cadre juridique établi par le traité de Lisbonne et la Charte des droits fondamentaux de l'Union européenne, désormais contraignante, et renouvelle les demandes exprimées dans sa résolution du 17 septembre 2009, notamment aux paragraphes 7 à 13;
 3. charge son Président de transmettre la position du Parlement au Conseil, à la Commission, aux gouvernements et aux parlements des États membres, ainsi qu'au gouvernement des États-Unis d'Amérique.

¹ Textes adoptés, P7_TA-PROV(2009)0016.

EXPOSÉ DES MOTIFS

1. Rappel de l'histoire

À la suite des attentats terroristes du 11 septembre 2001, le département du Trésor américain a développé le programme de surveillance du financement du terrorisme (TFTP), en vertu duquel il demandait, au moyen d'injonctions administratives, à SWIFT¹ de transférer certaines données de messagerie financière. Un grand nombre de ces données proviennent des États membres de l'Union européenne.

Vers le milieu de l'année 2006, les médias ont révélé l'existence du TFTP, déclenchant une controverse importante au sein de l'UE. À la suite de cela, le Conseil et la Commission ont engagé des discussions avec le département du Trésor américain au début de l'année 2007. À la suite de ces discussions, le département du Trésor américain a pris, à l'égard de l'UE, une série d'engagements unilatéraux en juin 2007 (dans lesdites observations relatives au TFTP).

En mars 2008, la Commission a annoncé qu'elle avait désigné le magistrat Jean-Louis Bruguière comme "éminence" européenne chargée de vérifier le respect par les États-Unis de ces observations. Le premier rapport a été publié en décembre 2008. Le juge Bruguière vient juste de présenter son second rapport final. Votre rapporteure en a reçu une copie (rapport classé "restreint UE") le lundi 1^{er} février 2010.

Jusqu'à récemment, SWIFT sauvegardait les messages sur deux serveurs identiques ("miroir") afin d'améliorer la faculté de récupération des données, situées en Europe et aux États-Unis. Or, en octobre 2007, SWIFT a annoncé une nouvelle architecture en matière de messagerie, conformément à laquelle, à compter du 1^{er} janvier 2010, les données de messagerie intracommunautaires (y compris les messages échangés entre pays reliés à la zone européenne) seraient désormais exclusivement traitées et sauvegardées en Europe.

En ce qui concerne le TFTP, il en résulte qu'une partie importante des données qui formaient la base des injonctions du TFTP ne seront plus sauvegardées aux États-Unis, ces derniers n'ayant plus accès à une partie importante des données qu'ils recevaient conformément à l'ancienne architecture.

À la suite d'une demande des États-Unis, le Conseil a décidé de négocier un accord international (intérimaire). Le 30 novembre 2009, le Conseil a signé un accord UE-US intérimaire sur le traitement et le transfert de données de messagerie financière aux fins du TFTP américain (FMDA) devant être appliqué provisoirement à compter du 1^{er} février 2010 jusqu'au 31 octobre 2010 au plus tard.

Conformément aux dispositions du traité de Lisbonne, l'accord du Parlement européen est nécessaire à la conclusion formelle de cet accord intérimaire. Que le Parlement européen

¹ La société "Society for Worldwide Interbank Financial Telecommunication" (SWIFT), de droit belge, est un fournisseur de messages sécurisés pour les transactions financières, avec environ 8500 clients, dont environ 7800 sont des institutions financières.

donne son accord ou pas, il ne sera pas possible de renégocier, étant donné que l'accord international a déjà été signé.

2. L'importance de la coopération transatlantique pour la lutte contre le terrorisme

Il convient avant tout de préciser que votre rapporteure soutient une UE ouverte, démocratique, forte, atlantiste, tournée vers l'extérieur et capable d'agir en coopération étroite avec les États-Unis, sur un pied d'égalité, et non pas comme un contrepoids. Sans aucun doute, l'UE et les États-Unis sont plus proches l'un de l'autre que de n'importe quel autre acteur international majeur.

Votre rapporteure tient à rappeler que le Parlement avait accueilli favorablement la "déclaration de Washington" (28 octobre 2009) sur le renforcement de la coopération transatlantique dans le domaine de la justice, de la liberté et de la sécurité dans un contexte de respect des droits de l'homme et des libertés civiles, et insiste fortement sur la nécessité de la coopération transatlantique. Elle souligne la nécessité de poursuivre et de renforcer la coopération entre les législateurs des États-Unis et de l'UE sur des questions d'intérêt commun et est convaincue que le cadre de la coopération transatlantique en vue de la lutte contre le terrorisme devrait être encore développé et amélioré.

Depuis le 11 septembre 2001, l'UE et les États-Unis ont négocié plusieurs accords couvrant les questions de JAI. Chaque accord a été négocié individuellement, avec de nombreux problèmes similaires à chaque fois, notamment en ce qui concerne les données à caractère personnel et la protection juridique. Pour surmonter ces difficultés récurrentes, le Parlement a demandé (depuis 2003) la définition d'un cadre juridique cohérent au niveau de l'UE pour la protection des données ainsi que la négociation d'un accord transatlantique contraignant dans ce domaine.

Le 6 novembre 2006, un groupe de contact à haut niveau UE-US a été mis en place afin de discuter du respect de la vie privée et de la protection des données à caractère personnel dans le contexte de l'échange d'informations pour répondre aux besoins des services répressifs, au sein d'une réflexion plus large entre l'UE et les États-Unis sur la meilleure façon de prévenir le terrorisme et la grande criminalité transnationale et de lutter contre ces phénomènes. Le 28 mai 2008, le groupe a remis son rapport final, établissant des principes généraux. Lors de la réunion des ministres de la Justice et des affaires intérieures UE-US du 12 décembre 2008, une large gamme de principes communs ainsi que certaines questions en suspens concernant le respect de la vie privée et la protection des données à caractère personnel ont été recensés, et il a été retenu comme objectif commun de commencer dès que possible les négociations sur un accord international contraignant.

Votre rapporteure est d'avis qu'il est d'une importance fondamentale d'obtenir un accord international contraignant et non pas une simple liste de principes si l'on veut que cet accord ait une quelconque valeur ajoutée. L'accord doit s'appliquer à des demandes individuelles et le cas échéant, aux transferts automatiques de masse. De plus, la déclaration de décembre 2008 est seulement un engagement politique et devra être suivie d'actes. Conformément au programme de Stockholm, adopté le 10 décembre 2009, les négociations sur un accord international contraignant devraient commencer dans les prochains mois.

En ce qui concerne le TFTP, la façon dont les services répressifs pourraient obtenir des données financières d'individus dans le cadre de leurs activités de répression, à savoir par l'intermédiaire de mandats ou d'injonctions individuels, approuvés par un tribunal, leur permettant d'examiner des transactions spécifiques au lieu de dépendre de larges injonctions administratives pour des millions d'enregistrements de données, doit être considérée comme un éloignement du droit européen et de la pratique en vigueur.

Comme mentionné plus tôt, la divulgation du programme (par les médias américains vers le milieu de l'année 2006) a conduit de façon compréhensible à une tempête de protestations au sein de l'UE, notamment parce que le TFTP ne semblait pas respecter les obligations fixées dans la directive sur la protection des données (95/46/CE) ainsi que les lois des États membres mettant en œuvre cette directive.

De plus, ce qui avait été lancé comme une mesure temporaire urgente (après le 11 septembre 2001) est devenu de facto une mesure permanente, sans autorisation spécifique des autorités de l'UE, ni véritable évaluation transatlantique de ses incidences, ni négociations transatlantiques couvrant en même temps les questions de sécurité, de coopération judiciaire et de protection des données. Cette façon de procéder n'a pas franchement contribué à instaurer une confiance mutuelle dans la coopération transatlantique pour la lutte contre le terrorisme.

On ne peut pas nier qu'avec l'accord intérimaire sur le traitement et le transfert des données de messagerie financière (FMDA), l'UE continue à externaliser ses services de renseignements financiers aux États-Unis. À cet égard, votre rapporteure convient avec SWIFT que le débat actuel ne concerne pas SWIFT en tant que telle, mais la façon dont l'Europe pourrait coopérer avec les États-Unis en vue de la lutte contre le terrorisme et la façon dont on demande aux fournisseurs de données de messagerie financière de contribuer à cette lutte, ou de façon plus générale, la question de l'utilisation – à des fins répressives – de données collectées à des fins commerciales.

Elle estime également qu'on ne peut pas transiger sur les exigences légales applicables au traitement équitable, proportionné et licite des informations personnelles et que l'UE et ses États membres n'ont jusqu'à présent pas suffisamment été fermes et clairs pour fixer leurs propres objectifs.

Enfin, il n'est pas difficile d'imaginer que le fait d'accepter l'accord proposé (dans sa version actuelle) pourrait conduire à accepter d'autres demandes de données commerciales, avec par exemple Skype, PayPal et d'autres entreprises du secteur de l'information et des télécommunications devenant potentiellement intéressantes pour les besoins des services répressifs.

3. Considérations juridiques liées à l'accord FMDA (non exhaustives)

Gardant à l'esprit les principaux éléments de la résolution du Parlement européen du 17 septembre 2009 sur le sujet, votre rapporteure souhaite faire les remarques suivantes sur le texte de l'accord.

Le principe de proportionnalité: SWIFT ne peut pas, pour des raisons techniques et de

gouvernance, rechercher le contenu des messages et ne peut donc pas rechercher des données sur la base de critères tels que des noms, des adresses et/ou des numéros de facture d'individus. Par conséquent, si SWIFT recevait (Article 4 de l'accord FMDA) une demande de produire des données liées par exemple à un individu, SWIFT ne serait pas en mesure de produire ces données spécifiques pour des raisons techniques. À la place, SWIFT pourrait produire des "données en masse". Ces messages pourraient éventuellement contenir les données spécifiques (c'est-à-dire le nom ou l'adresse d'un individu) dont l'autorité a besoin pour lutter contre le terrorisme. La nature même de SWIFT ne permet donc pas de soumettre des demandes limitées.

Ce qui précède implique que SWIFT doit transmettre toutes – ou pratiquement toutes – ses données aux États-Unis. Ceci va à l'encontre des principes de base de la loi sur la protection des données, à savoir les principes de nécessité et de proportionnalité. Cela ne peut pas être rectifié ultérieurement par des mécanismes de surveillance et de contrôle.

NB: les règles de l'UE relatives à la poursuite des activités de financement du terrorisme sont basées sur la dénonciation des transactions douteuses ou irrégulières par des opérateurs financiers individuels.

En fait, il vaudrait mieux autoriser SWIFT à se doter de l'équipement nécessaire pour faire elle-même des recherches ciblées dans les données qu'elle stocke et traite, plutôt que toutes ses données ne soient transférées en masse aux États-Unis. Cela maintiendrait également le parallèle avec ce que l'UE fait dans le domaine de la conservation des données par les fournisseurs de services de télécommunication.

L'accord FMDA ne prévoit pas expressément que les demandes de transfert soient limitées dans le temps. De même, l'accord ne prévoit pas non plus expressément que les demandes de transfert soient soumises à une autorisation judiciaire et ne définit pas non plus suffisamment les conditions de l'échange de données TFTP entre les États-Unis et des pays tiers. Le contrôle public et la surveillance de l'accès des autorités aux données de SWIFT ne sont pas définies, même si le fonctionnement de l'accord FMDA est soumis au contrôle des comités de surveillance du Congrès américain.

L'accord prévoit que toutes les données non extraites soient effacées après un certain délai. Toutefois, les données extraites sont conservées pendant la durée applicable à l'autorité publique concernée. L'accord ne fournit aucune précision sur ces durées de conservation.

Les droits d'accès, de rectification, de compensation et de recours de la personne concernée à l'extérieur de l'UE ne sont pas définis de façon appropriée.

L'accord ne garantit pas aux citoyens et entreprises européens les mêmes droits et garanties au titre de la législation américaine que ceux dont ils bénéficieraient sur le territoire de l'UE. De plus, l'accord ne précise pas dans quelles circonstances un individu ou une entreprise à l'extérieur du territoire des États-Unis doit être informé(e) du fait qu'une décision administrative défavorable a été prise contre lui/elle.

Même si le Conseil insiste pour dire qu'il est dans l'intérêt de l'UE d'assurer la durabilité du programme de surveillance du financement du terrorisme, nonobstant la nouvelle architecture

de SWIFT, et de garantir ainsi la sécurité juridique pour le transfert des données pertinentes au ministère du Trésor des États-Unis, étant donné que les services des États membres ont été les principaux bénéficiaires des indices tirés du TFTP, il est impossible de revendiquer une réelle réciprocité. Une réelle réciprocité impliquerait que les autorités américaines permettent aux autorités européennes d'obtenir et d'utiliser des données de messagerie financière et des données apparentées sauvegardées sur des serveurs aux États-Unis.

De plus, par rapport à l'accord proposé, le Conseil n'a pas précisé le rôle exact de l'"autorité publique" à laquelle incombera la responsabilité d'instruire les requêtes du Trésor des États-Unis (en particulier la nature des pouvoirs dont cette "autorité" sera investie ainsi que les voies et moyens de faire appliquer ces pouvoirs).

L'expression "n'est pas censé déroger à" (article 13 de l'accord) ne correspond à aucune disposition du traité ou terme consacré dans le droit européen, et sa signification est franchement obscure.

4. Relations interinstitutionnelles

En demandant l'approbation du Parlement pour la conclusion de l'accord sur le traitement et le transfert de données de messagerie financière dans des conditions dans lesquelles il était impossible au Parlement de réagir, pour des raisons pratiques, avant l'application provisoire de l'accord, le Conseil a en fait fixé au Parlement un délai contraire à l'esprit de l'article 218, paragraphe 6, point a) du traité sur le fonctionnement de l'UE et en partie sapé l'effet juridique et les incidences pratiques de la décision du Parlement dans le cadre de la procédure d'approbation, notamment en ce qui concerne son application provisoire.

Les informations sur la mise en œuvre de l'accord sont directement pertinentes pour les négociations et la conclusion de l'accord à long terme prévu à l'article 15, paragraphe 4, de l'accord, et le Parlement est par conséquent en droit d'avoir accès à ces informations.

Il devrait être clair que le Parlement doit être entièrement et immédiatement informé à tous les stades de la procédure. La raison d'être d'un tel devoir d'information n'est pas de permettre au Parlement de prendre note passivement des actions des autres institutions mais de lui donner la possibilité d'exercer une certaine influence sur la Commission et le Conseil en ce qui concerne le contenu de l'accord, afin de faciliter son approbation du texte final. L'obligation d'information parlementaire reflète en outre le devoir plus général des institutions de pratiquer entre elles une coopération loyale.

Toutes les informations et tous les documents pertinents doivent par conséquent être mis à la disposition des délibérations du Parlement, y compris l'avis du service juridique du Conseil et les renseignements à la base des deux rapports du juge Jean-Louis Bruguière (conformément aux règles applicables en matière de confidentialité).

5. Scénario possible après le refus de l'avis conforme

Si le Parlement refuse son avis conforme, l'accord sur le traitement et le transfert de données de messagerie financière n'entrera pas en vigueur et son application provisoire prendra fin dès notification de l'UE aux autorités américaines.

La façon la plus évidente de continuer l'échange de données serait dans le cadre de l'accord UE-US relatif à l'entraide judiciaire, un instrument plus général que l'accord sur le traitement et le transfert de données de messagerie financière. Pour les États membres qui ont un accord bilatéral avec les États-Unis en matière d'entraide judiciaire, l'accord UE-US relatif à l'entraide judiciaire complètera plus qu'il ne remplacera l'accord bilatéral.

Cet accord n'est pas limité aux infractions terroristes; en ce qui concerne les demandes d'informations bancaires, il suffit que la demande concerne une personne physique ou morale identifiée, soupçonnée ou accusée d'une infraction pénale, même si l'État concerné peut limiter les catégories des infractions au sujet desquelles il fournira une aide judiciaire. Les informations peuvent contenir des enregistrements de "comptes ou transactions" bancaires spécifiques détenus par des banques ou des institutions financières non bancaires. La demande d'information doit notamment identifier la personne, indiquer pour quels motifs elle est soupçonnée d'avoir commis un délit et montrer comment ces informations sont liées à l'enquête ou à la procédure pénale.

Le transfert de données aux États-Unis sera régi par la loi de l'État membre concerné.

6. Recommandation relative à l'accord et voie à suivre

Sur la base de ce qui précède, votre rapporteure recommande au Parlement de refuser son avis conforme.

Elle compte toutefois sur le Conseil et la Commission pour faire avancer de façon rapide et ambitieuse la stratégie européenne dynamique de lutte contre le terrorisme. La sécurité des citoyens européens ne saurait être mise en danger, ni la protection des données des citoyens, la sécurité du cadre juridique au sein duquel opèrent les entreprises ou encore les règles du jeu commerciales. Il doit rester clair à tout moment qu'il s'agit d'une responsabilité européenne et qu'une solution européenne doit être trouvée. Les Pays-Bas et la Belgique ne peuvent pas se retrouver les dupes de tout cela.

L'échange et l'utilisation ciblés de données dans le cadre de la lutte contre le terrorisme sont nécessaires et le resteront. Chercher les failles en matière de sécurité devrait être au centre de nos préoccupations. L'importance de la collecte de renseignements va de soi. Et la même chose est valable pour l'intégration et l'interprétation des renseignements collectés. Le public doit avoir confiance à la fois dans le traitement des données et dans les exigences de sécurité. L'objectif devrait être de trouver la bonne solution du premier coup.

Le Parlement européen demande à la Commission de présenter des recommandations pour l'ouverture immédiate de (nouvelles) négociations avec les États-Unis à la fois sur les données de messagerie financière à des fins d'enquêtes antiterroristes et sur la protection de la vie privée/des données personnelles dans le contexte de l'échange d'information pour répondre aux besoins des services répressifs.

Il demande au Conseil, en réponse, d'exprimer son point de vue sur le contenu des directives en matière de négociation qu'il adoptera à la suite de ces recommandations. Il est évident que l'on s'attend à ce que les préoccupations et les recommandations du Parlement européen, ainsi

que du contrôleur européen de la protection des données et du groupe de travail "Article 9" soient prises en compte.

Il demande également au Conseil et à la Commission d'envisager une solution qui pourrait compléter (et éventuellement même remplacer) le traité d'entraide judiciaire entre les États-Unis et l'Union européenne, par exemple en exposant les implications de l'échange d'information qui est essentiellement basé sur les renseignements plutôt qu'un exemple d'informations échangées au titre de la coopération ordinaire en matière d'entraide judiciaire. En examinant une telle stratégie, il convient d'accorder une attention particulière à la recherche d'une solution européenne pour la surveillance de l'échange de données, c'est-à-dire déterminer une autorité (judiciaire) indépendante de l'UE qui serait chargée de vérifier les opérations du TFTP (et même de bloquer le système du TFTP). La condition préalable nécessaire à cette solution européenne est un accord international contraignant sur la protection de la vie privée et des données à caractère personnel dans le contexte de l'échange d'information pour répondre aux besoins des services répressifs.

Il pourrait être utile d'inviter le Groupe d'action financière internationale (GAFI) à présenter également des recommandations.

RÉSULTAT DU VOTE FINAL EN COMMISSION

Date de l'adoption	4.2.2010
Résultat du vote final	+: 29 -: 23 0: 1
Membres présents au moment du vote final	Jan Philipp Albrecht, Sonia Alfano, Louis Bontes, Mario Borghezio, Rita Borsellino, Emine Bozkurt, Simon Busuttil, Philip Claeys, Carlos Coelho, Rosario Crocetta, Cornelis de Jong, Agustín Díaz de Mera García Consuegra, Cornelia Ernst, Tanja Fajon, Kinga Göncz, Nathalie Griesbeck, Sylvie Guillaume, Ágnes Hankiss, Jeanine Hennis-Plasschaert, Salvatore Iacolino, Sophia in 't Veld, Livia Járóka, Teresa Jiménez-Becerril Barrio, Timothy Kirkhope, Juan Fernando López Aguilar, Monica Luisa Macovei, Clemente Mastella, Nuno Melo, Louis Michel, Claude Moraes, Antigoni Papadopoulou, Georgios Papanikolaou, Jacek Protasiewicz, Carmen Romero López, Birgit Sippel, Renate Sommer, Rui Tavares, Wim van de Camp, Axel Voss, Manfred Weber, Renate Weber, Tatjana Ždanoka
Suppléant(s) présent(s) au moment du vote final	Alexander Alvaro, Elena Oana Antonescu, Andrew Henry William Brons, Ioan Enciu, Ana Gomes, Jean Lambert, Petru Constantin Luhan, Raúl Romeva i Rueda, Michèle Striffler
Suppléant(s) (art. 187, par. 2) présent(s) au moment du vote final	Françoise Grossetête, Marita Ulvskog