

Accord UE/États-Unis: traitement et le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme

2010/0178(NLE) - 24/06/2010 - Document de base législatif

OBJECTIF: **conclure** un nouvel accord entre l'Union européenne et les USA sur le traitement et le transfert de données de messagerie financière de l'UE aux USA aux fins du programme de surveillance du financement du terrorisme (ou TFTP).

ACTE PROPOSÉ : Décision du Conseil

ANALYSE D'IMPACT : aucune analyse d'impact n'a été réalisée

BASE JURIDIQUE : article 87, par. 2, point a), et article 88, par. 2, en liaison avec article 218, par. 6, point a) du traité sur le fonctionnement de l'Union européenne (TFUE).

CONTENU : le présent document reprend le texte du nouvel accord entre l'UE et les USA 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.

Largement inspiré de [sa version antérieure](#), les principaux éléments de cet accord peuvent se résumer comme suit :

Objet de l'accord : comme dans sa précédente version, l'objectif de l'accord est de garantir, dans le respect intégral de la vie privée, de la protection des données à caractère personnel, et d'autres conditions énoncées à l'accord que:

-) les données de messagerie financière faisant référence à des transferts financiers et les données connexes qui sont stockées sur le territoire de l'UE par les fournisseurs de services de messagerie financière internationale désignés conjointement en vertu de l'accord, sont fournies au département du Trésor des États-Unis, exclusivement aux fins de la prévention et de la détection du terrorisme ou de son financement, ainsi que des enquêtes ou des poursuites en la matière; et
-) les informations pertinentes obtenues grâce au TFTP sont mises à la disposition des services répressifs, des organismes chargés de la sécurité publique ou des autorités chargées de la lutte contre le terrorisme des États membres, ou d'EUROPOL ou EUROJUST, aux fins de la prévention et de la détection du terrorisme ou de son financement, ainsi que des enquêtes ou des poursuites en la matière.

Données concernées : il s'agit des données de messagerie financière et de données connexes portant sur les actes d'une personne ou d'une entité qui présentent un caractère violent, un danger pour la vie humaine ou qui font peser un risque de dommage à des biens ou à des infrastructures, et qui, compte tenu de leur nature peuvent être raisonnablement perçus comme étant perpétrés dans le but:

- d'intimider une population ou faire pression sur elle;
- d'intimider ou de contraindre des pouvoirs publics ou une organisation internationale, ou

- de déstabiliser gravement ou détruire les structures fondamentales politiques, constitutionnelles, économiques ou sociales d'un pays ou d'une organisation internationale.

Il peut également s'agir de données émanant d'une personne ou une entité qui facilite ou favorise les actes ci-avant décrits, y contribue financièrement, matériellement ou techniquement, ou qui aide à les commettre ou s'en rend complice.

Garantir la fourniture des données par les fournisseurs désignés : l'UE devra veiller à ce que les entités désignées par les parties comme fournisseurs de services de messagerie financière internationale (les "fournisseurs désignés" en vertu de l'accord à savoir la Société de télécommunications financières interbancaires mondiales ou *Society for Worldwide Interbank Financial Telecommunication* - SWIFT) fournissent au département américain du Trésor les données de messagerie financière et les données connexes demandées par celui-ci aux fins de la prévention et de la détection du terrorisme ou de son financement, ainsi que des enquêtes en la matière (les "données fournies").

Demandes des USA visant à obtenir des données SWIFT : une procédure est prévue pour déterminer la méthode d'obtention des informations recherchées à destination du département américain du Trésor. En principe, ce dernier devra produire une demande dans le but d'obtenir les données nécessaires aux fins de la prévention et de la détection du terrorisme ou de son financement, ainsi que des enquêtes ou des poursuites en la matière, stockées sur le territoire de l'UE.

La demande (accompagnée d'éventuels documents complémentaires) devra :

- identifier aussi clairement que possible les données, y compris les catégories spécifiques de données demandées;
- expliquer en quoi elles sont nécessaires;
- **réduire au maximum le volume des données demandées**, compte tenu des analyses du risque terroriste passé et présent,
- ne pas porter sur des données liées à l'espace unique de paiements en euros.

Toute demande devra faire l'objet d'une copie à EUROPOL. Des dispositions sont en outre prévues pour strictement encadrer la réponse de SWIFT en direction du département du Trésor des États-Unis.

Garanties applicables au traitement des données fournies : le département américain du Trésor devra prendre les mesures nécessaires pour que les données fournies soient traitées conformément aux dispositions de l'accord, à savoir, en obéissant à des dispositions destinées à **éviter toute forme d'exploration des données par profilage algorithmique ou informatisé, ou tout autre type de filtrage**. Le Trésor américain devra s'engager à protéger les données visées par l'accord sans discrimination fondée sur la nationalité ou le pays de résidence, et en appliquant une série de mesures spécifiques de sauvegarde détaillées à l'accord. Ces mesures visent globalement à faire en sorte que **les données fournies** font l'objet d'un **traitement sûr et intègre**.

Traitement nécessaire et proportionné des données : des dispositions sont prévues en vue de garantir que les recherches effectuées sur les données laissent à penser que les informations fournies **ont un lien avec le terrorisme ou son financement**. Les données peuvent comprendre des informations d'identification sur l'émetteur et/ou le bénéficiaire de l'opération, comme le nom, le numéro de compte, l'adresse et le numéro national d'identification. Une attention particulière devra être accordée au traitement des données touchant à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou autres, ou l'appartenance à un syndicat, ou relatives à la santé ou à la vie sexuelle (les "données sensibles"). En tout état de cause ces données devront être protégées comme il convient par le département du Trésor américain.

Conservation et effacement de données : au cours de la période durant laquelle l'accord restera en vigueur, le département américain du Trésor devra évaluer en permanence (et au moins une fois par an) que les données non extraites qui ne sont plus nécessaires pour lutter contre le terrorisme ou son financement sont identifiées. Celles-ci devront alors être effacées dès que cela sera techniquement possible. En principe, toutes les données non extraites reçues avant le 20 juillet 2007 devront être effacées au plus tard le 20 juillet 2012. Les données reçues après cette date devront être effacées au plus tard 5 ans après leur réception. Au plus tard 3 ans après la date d'entrée en vigueur de l'accord, la Commission et le département américain du Trésor devront établir un rapport conjoint relatif à la valeur des données fournies dans le cadre de l'accord.

Transfert ultérieur : des dispositions sont prévues en vue du transfert ultérieur d'informations extraites des données fournies mais dans un cadre limité et strictement réglementé. En toute état de cause, ces informations ne seront partagées qu'uniquement dans un but de recherche d'indices et aux seules fins de la prévention et de la détection du terrorisme ou de son financement. Lorsque le département américain du Trésor sait que ces informations concernent un citoyen ou un résident d'un État membre, tout partage de ces informations avec les autorités d'un pays tiers est soumis à l'accord préalable des autorités compétentes de l'État membre concerné.

Communication spontanée d'informations : le département américain du Trésor devra veiller à mettre le plus rapidement possible à la disposition des services répressifs, des organismes chargés de la sécurité publique ou des autorités chargées de la lutte contre le terrorisme des États membres ainsi que d'EUROPOL et EUROJUST, toute information obtenue dans le cadre du TFTP qui pourrait contribuer, dans l'Union, à la prévention et à la détection du terrorisme ou de son financement. Toute information obtenue dans ce contexte et susceptible de contribuer, aux États-Unis, à la prévention et à la détection du terrorisme ou de son financement devra être communiquée en retour aux USA sur une base réciproque.

Demandes de recherches TFTP émanant de l'UE : lorsqu'un service répressif ou un organisme équivalent chargé de la lutte contre le terrorisme dans un État membre, EUROPOL ou EUROJUST, établit qu'il y a lieu de penser qu'une personne ou une entité a un lien avec le terrorisme, il peut demander une recherche d'informations pertinentes obtenues dans le cadre du TFTP. Cette recherche est effectuée par le département américain du Trésor sans délai.

Coopération avec un futur système équivalent de l'UE : pendant la durée de validité de l'accord, la Commission réalisera une étude au sujet de l'éventuelle introduction d'un système équivalent propre à l'UE permettant un transfert plus ciblé de données. Si, à la suite de cette étude, l'UE décide de mettre en place un système propre, les États-Unis devront coopérer et offrir conseils et assistance à la mise en place effective d'un tel système. Le cas échéant, le présent accord fera l'objet d'une modification.

Suivi des garanties et contrôles : le respect de la limitation stricte à l'objectif de lutte contre le terrorisme ainsi que des autres garanties prévues à l'accord fait l'objet d'un contrôle et d'un suivi par des contrôleurs indépendants, y compris par une personnalité désignée par la Commission en accord avec les États-Unis. Ces contrôles impliquent le pouvoir de réexaminer en temps réel et rétrospectivement toutes les recherches effectuées sur les données fournies, et, le cas échéant, de demander une justification complémentaire du lien avec le terrorisme. En particulier, les contrôleurs indépendants ont le pouvoir de bloquer tout ou partie des recherches qui apparaissent être en violation de l'accord.

Réexamen conjoint : à la demande d'une des parties et en tout état de cause après un délai de 6 mois à compter de la date d'entrée en vigueur de l'accord, les parties devront conjointement réexaminer les dispositions en matière de garanties, de contrôles et de réciprocité de l'accord. À la suite de ce réexamen, la Commission présentera un rapport au Parlement européen et au Conseil sur le fonctionnement global de l'accord.

Transparence : pour garantir la transparence du fonctionnement de l'accord, le département du Trésor américain devra publier sur son site internet (accessible au public) des informations détaillées au sujet du TFTP et de ses finalités, y compris les coordonnées des personnes à contacter pour obtenir des renseignements complémentaires sur les procédures de recours administratifs et judiciaires applicables aux États-Unis.

Droit d'accès : des dispositions sont prévues pour garantir que les droits en matière de protection des données ont été respectés et que toute personne puisse accéder à ses données. La communication de ces données sera subordonnée à **des restrictions légales raisonnables** afin de ne pas compromettre la prévention, la détection, la recherche et la poursuite d'infractions pénales, et de protéger la sécurité publique ou la sécurité nationale, tout en tenant dûment compte de l'intérêt légitime de la personne concernée. Lorsque l'accès aux données à caractère personnel est refusé ou limité, ce refus ou cette limitation devra être expliqué par écrit et des informations devront être fournies quant aux moyens disponibles pour former un recours administratif ou judiciaire aux États-Unis.

Droit de rectification, d'effacement ou de verrouillage : il est prévu que toute personne puisse rectifier, effacer ou verrouiller ses données à caractère personnel traitées par le département américain du Trésor lorsqu'elle constate que ces données sont inexactes ou lorsque le traitement est contraire à l'accord. Une procédure est prévue à cet effet. Des dispositions sont également prévues afin de garantir que les données reçues ou transmises puissent être complétées, supprimées ou corrigées.

Recours : des dispositions spécifiques sont prévues en matière recours. Ainsi, toute personne estimant que des données à caractère personnel la concernant ont fait l'objet d'un traitement en violation de l'accord aura un droit de recours administratif ou judiciaire effectif en application de la législation de l'UE, de ses États membres et des États-Unis, respectivement. À cette fin, le département américain du Trésor devra accorder à toute personne un traitement équitable lors de l'application de ses procédures administratives, **indépendamment de la nationalité ou du pays de résidence**.

Consultation : il est prévu que les parties se consultent pour permettre une utilisation aussi efficace que possible de l'accord, et pour favoriser le règlement de tout différend concernant son interprétation ou son application. Les parties sont notamment appelées à se consulter immédiatement dans le cas où un tiers, y compris une autorité d'un autre pays, conteste tout aspect relatif aux effets ou à la mise en œuvre de l'accord ou forme un recours juridique à cet égard.

Suspension ou dénonciation : l'accord peut faire l'objet d'une dénonciation ou d'une suspension, en cas de violation de ses obligations. Les parties sont appelées à se consulter dans ce cas afin de trouver une solution mutuellement acceptable.

Dispositions territoriales : l'accord ne s'appliquera au Danemark, au Royaume-Uni, ou à l'Irlande que si la Commission notifie par écrit aux États-Unis que le Danemark, le Royaume-Uni, ou l'Irlande ont choisi d'être liés à l'accord, selon des modalités spécifiques d'application.

INCIDENCE BUDGÉTAIRE : la proposition n'a pas d'incidence sur le budget de l'UE.