COMMISSION
EUROPÉENNE

Bruxelles, le 27.11.2013
SWD(2013) 489 final

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant le document:

Communication de la Commission européenne au Parlement européen et au Conseil relative à un système européen de surveillance du financement du terrorisme («TFTS»)

{COM(2013) 842 final}
{SWD(2013) 488 final}

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

RÉSUMÉ DE L'ANALYSE D'IMPACT

accompagnant le document

Communication de la Commission européenne au Parlement européen et au Conseil relative à un système européen de surveillance du financement du terrorisme («TFTS»)

1. INTRODUCTION

En 2010, lorsque l'UE a conclu l'accord entre l'Union européenne et les États-Unis 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 (accord TFTP UE-États-Unis), le Conseil et le Parlement européen ont invité la Commission à rechercher un système similaire qui permettrait l'extraction de ces données sur le territoire de l'UE. L'accord TFTP UE-États-Unis fait allusion à un tel système européen dans l'un de ses articles, en mentionnant que la Commission européenne réalisera une étude au sujet de l'introduction d'un système équivalent propre à l'UE.

Compte tenu de la complexité juridique et technique de la question et de sa sensibilité due à son incidence sur les droits fondamentaux, notamment la protection des données à caractère personnel, la Commission a décidé de publier, en juillet 2011, une communication présentant diverses options, afin d'exposer les formes que pourrait prendre la création d'un tel système.

Les discussions ultérieures et le retour d'informations n'ont révélé aucune préférence nette des États membres ou du Parlement européen pour l'une ou l'autre option. C'est pourquoi la Commission a décidé de passer toutes les options en revue dans la présente analyse d'impact et de les détailler en développant différentes sous-options.

Depuis l'époque où la Commission avait été invitée à proposer un cadre pour un système européen de surveillance du financement du terrorisme (SSFT), la situation économique s'est

modifiée dans l'Union et dans les États membres, et ceux-ci comprennent mieux désormais le bénéfice qu'ils peuvent tirer des échanges de données au titre de l'accord TFTP UE-États-Unis, grâce aux clauses de réciprocité qu'il comporte. Il a été tenu compte de ces évolutions et de ces facteurs lorsque les options envisageables pour l'introduction d'un nouveau système ont été comparées à celle du maintien du statu quo, car ce statu quo a changé depuis 2010.

2. DEFINITION DU PROBLEME

Du fait de sa nature transnationale, le financement du terrorisme est très difficile à détecter et à combattre

Selon le dernier rapport TE-SAT 2012 d'Europol, les États membres continuent à faire face à une grave menace terroriste, qu'il s'agisse de terrorisme islamiste ou d'inspiration religieuse, ethno-nationaliste et séparatiste, de gauche ou de droite, ou de terrorisme anarchiste. Afin de priver les terroristes de leur capacité à se livrer à leurs activités, une composante essentielle de la stratégie antiterroriste de l'UE consiste à empêcher les terroristes et les organisations de récolter des fonds, de les transférer et d'y avoir accès. Lutter contre le financement du terrorisme signifie empêcher le soutien financier à ce dernier ou à ceux qui l'encouragent, qui le planifient ou qui s'y livrent.

Les activités terroristes sont très souvent de nature transnationale. Non seulement elles englobent des activités qui sont planifiées dans un pays et exécutées dans un autre, mais elles impliquent des collectes de fonds et des transferts d'argent au-delà des frontières. Ces activités transnationales permettent aux terroristes de dissimuler la manière dont ils déplacent leur argent, ainsi que son origine et sa finalité. Du fait de la nature transnationale du financement du terrorisme, il est extrêmement difficile de le détecter et d'y mettre fin. La coopération internationale dans ce domaine revêt, dès lors, une importance capitale. C'est pourquoi l'UE a accepté de travailler de concert avec les États-Unis dans ce domaine, comme en témoigne plus particulièrement l'accord TFTP UE-États-Unis.

Outre les nombreux instruments législatifs, il existe également plusieurs organismes internationaux et de l'UE qui participent activement à la lutte contre le financement du terrorisme et qui encouragent la coopération internationale ou européenne. Il s'agit du Groupe d'action financière sur le blanchiment de capitaux et le financement du terrorisme (GAFI), du Comité sur la prévention du blanchiment de capitaux et du financement du terrorisme, des

cellules de renseignement financier (CRF) de l'UE, d'Eurojust et d'Europol. Divers instruments législatifs existent pour renforcer la coopération entre les États membres de l'UE, tels qu'une décision relative à la coopération entre les cellules de renseignement financier de l'UE.

Les mesures et instruments en vigueur sont inadaptés pour suivre la piste financière des terroristes

Même si la coopération entre les États membres de l'UE dans ce domaine s'améliore constamment, y compris la coopération consécutive à la création de nouveaux instruments juridiques tels que le mandat européen d'obtention de preuves, les échanges d'informations sur les données financières sont limités. Les instruments d'entraide judiciaire ou la coopération entre les cellules de renseignement financier de l'UE ne permettent pas, et n'ont pas pour finalité, d'établir un profil du suspect, de découvrir rapidement tous les comptes existants d'une personne soupçonnée et les opérations financières y afférentes (et ceux des entreprises et autres organisations à son nom), dans le monde entier, en remontant plusieurs années en arrière. En dehors du TFTP, il n'existe actuellement aucun instrument qui puisse produire des informations sur le suspect au tout début d'une enquête, dans un délai très court, permettant ainsi aux enquêteurs de se concentrer sur certaines catégories de transactions financières, sur certains pays et/ou sur une certaine période dans le temps, pour établir une chronologie précise des faits et gestes d'un suspect. Or le TFTP est un outil exclusivement exploité par les États-Unis, ce qui signifie qu'il sert avant tout leurs besoins en matière de sécurité.

Les facteurs sous-jacents au problème

1. **Le mécanisme actuellement en vigueur pour analyser les données de messagerie financière est dirigé par un pays tiers, ce qui ne va donc pas pleinement dans le sens des intérêts spécifiques de l'Union européenne.**

Dans l'Union, la menace terroriste provient essentiellement de séparatistes, de mouvements d'inspiration religieuse, de l'extrême gauche et l'extrême droite, et d'anarchistes. L'intensité de ces menaces et le risque qu'elles représentent semblent obéir à un cycle et, dans une certaine mesure, ces menaces sont tout à fait différentes de celle visant les États-Unis, essentiellement

liée au terrorisme islamiste, qui n'est pas présent aux États-Unis mêmes, ou seulement de manière limitée.

L’objectif premier du TFTP est d’enquêter sur les activités terroristes ayant trait à la menace telle qu'elle est perçue par les États-Unis. Néanmoins, de plus en plus d'États membres ont commencé à recourir aux clauses de réciprocité de l’accord pour bénéficier des échanges de données avec les autorités américaines. Dès lors, ce facteur évolue au fil du temps et son importance décroît au fur et à mesure que les États membres prennent l'habitude d'invoquer l'accord et de recourir au TFTP pour faire face aux menaces visant l’UE.

2. **Le mécanisme actuellement en vigueur pour analyser les données de messagerie financière ne comprend qu’un fournisseur dans ce domaine et qu'un type de message**

Étant donné qu’il s’agit d’un programme américain à vocation mondiale, à l’heure actuelle, seuls les messages FIN (Financial Institution Transfer) transférés par le réseau de la Society for Worldwide Interbank Financial Telecommunication (SWIFT) sont inclus dans le TFTP. Les messages FIN sont un type de message créé par SWIFT, par lequel des informations financières sont transmises d’un établissement financier à l’autre. Or, parallèlement aux transferts SWIFT, il existe de nombreux autres grands systèmes de transfert des paiements électroniques ainsi que divers autres fournisseurs sur le marché, tels que les chambres de compensation informatisées et les virements électroniques. Ils ne sont actuellement pas contrôlés par le TFTP et pourraient, dès lors, être utilisés par les terroristes ou par des entités liées au terrorisme pour transférer leurs fonds, sans être soumis à des contrôles.

3. **Le mécanisme actuellement en vigueur pour analyser les données de messagerie financière suscite des préoccupations quant à la protection de la vie privée et des données à caractère personnel des citoyens de l'Union**

La majorité des critiques porte sur la prétendue non-conformité du TFTP avec le droit au respect de la vie privée et familiale (article 7 de la Charte des droits fondamentaux) et le droit à la protection des données à caractère personnel (article 8 de la Charte et article 16 du TFUE), ainsi qu’avec les obligations prévues par la directive sur la protection des données (directive 95/46/CE). Des doutes ont été exprimés quant à la nécessité et la proportionnalité

de transférer des données relatives aux citoyens de l'UE vers un pays tiers, et quant aux procédures de vérification et d'autorisation permettant le transfert de ces données.

Par les deux réexamens conjoints de l'application de l'accord TFTP UE-États-Unis, les parties ont vérifié la bonne mise en œuvre des garanties détaillées figurant dans l'accord, y compris celles relatives à la protection des données à caractère personnel. L'application concrète et renouvelée de l'accord par l'Union européenne et par les États-Unis a replacé ce facteur dans son contexte, montrant que les préoccupations initiales sont aplanies par un ensemble de garanties effectives.

4. **En dehors de l'accord TFTP UE-États-Unis, l'Union et ses États membres ne disposent pas des moyens techniques et juridiques suffisants pour établir les liens financiers leur permettant de remonter jusqu'aux réseaux terroristes et d'en dégager le profil**

À l'échelle de l'UE, il n'existe pas de système distinct équivalent qui mettrait au jour les liens financiers permettant de remonter jusqu'aux réseaux terroristes et d'en dégager le profil. Les instruments législatifs et opérationnels en vigueur qui ont été mis en place au niveau de l'UE et des États membres, ou auxquels l'UE et les États membres prennent part (comme la plate-forme des CRF), ne présentent pas les mêmes avantages que le TFTP en matière de vitesse, d'efficience et d'efficacité; ils ne peuvent pas le faire et n'ont pas été conçus à cette fin. Dans le cadre du système préventif fondé sur la troisième directive antiblanchiment de capitaux, par exemple, les cellules de renseignement financier analysent des transactions financières au cas par cas, à la suite du signalement de transactions suspectes par les entités soumises à cette obligation, telles que les établissements financiers. Le système européen de gel des avoirs servant au financement des actions terroristes exige que soit officiellement dressée une liste, approuvée par le Conseil, de personnes et d'entités liées au terrorisme, afin d'empêcher les unes et les autres d'effectuer des transactions financières. Mais il n'existe aucun système d'exploitation de données qui pourrait mettre en évidence un schéma complet de «comportement» financier et les relations d'une personne ou d'une organisation soupçonnée de se livrer à des activités terroristes ou de les financer.

Le scénario de référence

Dans le cadre du scénario de référence, il ne serait créé, à ce stade, aucun système TFTP propre à l'UE. L'accord TFTP UE-États-Unis resterait en vigueur et continuerait de s'appliquer. Il n'y aurait qu'un seul fournisseur désigné tenu de divulguer les données financières pertinentes et seuls ses messages FIN seraient concernés. Les États membres ainsi qu'Europol et Eurojust continueraient de pouvoir invoquer la clause de réciprocité figurant dans l'accord TFTP UE-États-Unis. Cette clause permet aux autorités européennes d'obtenir directement des données financières pertinentes auprès du département du Trésor des États-Unis, données qui les aident à lutter plus efficacement dans l'Union contre le terrorisme et son financement. Le département du Trésor des États-Unis continuerait, en outre, d'envoyer spontanément des rapports sur d'éventuelles menaces terroristes aux États membres et à Europol, ainsi qu'il est prévu à l'article 9 de l'accord TFTP UE-États-Unis, sans avoir été saisi d'une demande particulière. Le niveau actuel de protection des données à caractère personnel serait maintenu sans que s'accroisse, simultanément, le volume des données collectées. Les parties ont, à deux reprises, réexaminé conjointement l'accord TFTP et ont vérifié le bon fonctionnement du programme et des mesures de contrôle rigoureuses qui avaient été adoptées pour que les garanties, dont celles relatives à la protection des données à caractère personnel, soient dûment respectées.

Le coût induit par l'instauration d'un nouveau système, comprenant à la fois l'investissement initial et les coûts de fonctionnement annuels, seraient évités. Il n'y aurait pas de risque supplémentaire pour les données à caractère personnel ni de niveau de risque variable à atténuer (à la différence de n'importe quelle option en faveur d'un système propre à l'UE).

3. OBJECTIFS ET OPTIONS

Objectifs

Les infractions terroristes causent de graves préjudices aux victimes, ainsi que des dommages économiques de grande ampleur, tout en sapant le sentiment de sécurité sans lequel les citoyens ne peuvent jouir effectivement de leur liberté et de leurs droits individuels. Un SSFT de l'UE aurait, dès lors, pour objectif global et principal de couper l'accès des terroristes aux sources de financement et de surveiller les transactions financières liées au terrorisme, afin de renforcer la sécurité dans l'UE.

Pour ce faire, la Commission a défini cinq objectifs spécifiques: veiller à ce que le système soit conçu pour répondre aux besoins de renseignements de l'UE en recourant aux évaluations de la menace réalisées à l'échelle de l'Union; entretenir une bonne coopération avec les États-Unis et d'autres pays tiers dans la lutte contre le terrorisme; veiller à ce que l'analyse des données de messagerie financière porte sur le(s) fournisseur(s) de services et le ou les types de message les plus concernés; assurer la pleine protection des droits au respect de la vie privée et à la protection des données des citoyens de l'Union lors du traitement de données de messagerie financière; et étendre l'accès de l'Union européenne et de ses États membres auxdites données, augmenter le nombre d'analyses de ces données et renforcer la capacité de l'Union et des États membres de mettre en évidence des liens entre des individus/groupes impliqués dans le terrorisme ou son financement. Les objectifs opérationnels rattachés aux facteurs sous-jacents au problème complètent le cadre dans lequel les différentes options ont été examinées.

Options

En ce qui concerne les options envisagées, l'analyse d'impact recense quatre niveaux d'options dont les deux premiers ont trait à la structure d'un système de surveillance, le troisième à la finalité de ce système et le quatrième, à la portée de celui-ci: «options excluant la création d'un SSFT propre à l'UE», «création d'un SSFT propre à l'UE avec différentes sous-options pour sa structure», «options relatives à la finalité d'un SSFT propre à l'UE» et «options relatives à la portée d'un SSFT propre à l'UE». À chaque niveau sont énumérées et détaillées plusieurs sous-options. Quatre sous-options ont été écartées car elles aggraveraient manifestement la situation actuelle, seraient tributaires de l'accord d'un pays tiers ou auraient des répercussions négatives non négligeables sur les budgets des États membres. Les options restantes sont les suivantes:

- le scénario de référence — statu quo

- les trois systèmes hybrides portant création d'un SSFT propre à l'UE, allant d'un très haut à un très faible niveau de participation de l'UE:

1. Le modèle consistant en un service de coordination et d'analyse SSFT de l'UE prévoit la création d'une unité centrale européenne du SSFT, dont la plupart des tâches et des fonctions seraient exécutées à l'échelle de l'UE. Les États membres pourraient

toutefois aussi effectuer leurs propres recherches par l'intermédiaire d'experts nationaux du SSFT qu'ils auraient désignés et qui seraient affectés au même endroit que l'unité européenne du SSFT.

2. Selon le modèle de service d'extraction SSFT de l'UE, il s'agirait de créer une unité centrale européenne du SSFT qui serait chargée d'adresser des demandes de données brutes à ou aux fournisseurs désignés. Les États membres auraient le droit de demander que des recherches soient effectuées pour leur compte.

3. Le modèle de coordination des CRF entraînerait la création d'une autorité ad hoc à l'échelle de l'UE, composée de toutes les CRF des États membres, et les tâches seraient réparties entre cette unité centrale et les CRF nationales;

- deux systèmes de conservation/ d'extraction:

1. le premier modèle serait un système de conservation dans lequel il serait demandé à ou aux fournisseurs désignés de conserver les données sur son/leur serveur pendant un certain temps.

2. La seconde option serait identique à la précédente, mais inclurait la création d'un dispositif de recherche dans les locaux du ou des fournisseurs désignés;

- deux options relatives à la finalité d'un SSFT propre à l'UE, l'une la limitant à la lutte contre le terrorisme, la seconde l'étendant aux formes graves de la criminalité organisée;

- deux options relatives à la portée d'un SSFT propre à l'Union: la première la limitant à l'actuel fournisseur désigné, SWIFT; la seconde comprenant de multiples fournisseurs désignés.

4. ANALYSE DES INCIDENCES

Les incidences économiques des options doivent reposer sur des estimations et des hypothèses. Il n'est, en effet, pas aisé de quantifier les éventuels avantages économiques, même si la Commission européenne sait pertinemment que, dans d'autres contextes, comme la santé par exemple, ce pourrait être fait en appliquant la méthodologie dite de «l'espérance de vie pondérée en fonction de la qualité de vie». En matière de terrorisme, toutefois, il semble impossible et disproportionné de tenter de chiffrer la valeur des vies humaines qui

pourraient être sauvées grâce à la prévention des attaques terroristes. Il est tout aussi impossible de prévoir très précisément les avantages économiques d'un système qui contribuerait à prévenir le terrorisme et les dommages qu'il cause à l'économie, ou à la propriété publique ou privée, car l'ampleur des attaques et les dégâts provoqués dépendent d'un grand nombre de variables imprévisibles. De même, il est difficile de quantifier l'impact social et psychologique 'des attentats terroristes.

Il convient, en outre, de rappeler que le mécanisme actuel est censé être un instrument de la politique de sécurité. Les données existantes dans ce contexte sont hautement confidentielles, afin d'empêcher les personnes ciblées par cet instrument d'être en mesure de le contourner ou d'adapter leurs comportements criminels et terroristes pour que le système ne soit pas ou plus en mesure de les détecter. Ce dernier point limite la possibilité de fournir, pour la présente analyse d'impact, le même degré de détail lorsque les incidences sont recensées, évaluées et comparées, que celui qui est d'usage pour des exercices similaires dans d'autres domaines d'action. Enfin, une part importante des informations utilisées pour réaliser l'analyse provient d'un pays tiers (les États-Unis) qui a une expérience pratique d'un système similaire de lutte contre le terrorisme et son financement. Parce qu'elles sont essentielles à la sécurité dans ce pays (les États-Unis), ces informations sont, dans une large mesure, classifiées. Même si ces informations ne peuvent pas être divulguées dans la présente analyse d'impact, la Commission européenne a été en mesure d'en examiner d'importants éléments dans son étude de la question en cause.

Quant aux coûts estimés pour les différentes options, un calcul détaillé est annexé à l'analyse d'impact. Outre l'impact économique, l'efficacité des différentes options (c'est-à-dire leur capacité d'atteindre les objectifs définis) constitue un autre volet important de l'incidence. De plus, pour chaque option, les répercussions sur les droits sociaux et les droits de l'homme ont été évaluées, ainsi que les retombées politiques, notamment l'effet sur les relations avec les pays tiers, en particulier les États-Unis. En ce qui concerne les autres incidences, l'analyse d'impact examine en détail la mesure dans laquelle l'option envisagée pourrait être concrétisée, et si elle serait acceptable pour les différentes parties prenantes et le public.

5. CONCLUSION

Après avoir défini et analysé les options envisageables pour la création d'un SSFT propre à l'UE et en avoir évalué les incidences, la Commission considère qu'à l'heure actuelle l'option privilégiée et la plus proportionnée consiste à maintenir le statu quo. Tout système de l'UE porterait atteinte à la protection des données et nécessiterait, dès lors, l'établissement de solides garanties et garde-fous en matière de protection des données. Il serait non seulement onéreux mais aussi lourd, sur les plans technique et opérationnel, de créer un tel système et d'en assurer la maintenance.

Le scénario de référence a évolué au fil du temps. Les États membres invoquent de plus en plus souvent les clauses de réciprocité et, grâce au transfert de données vers les États-Unis, ils renforcent la sécurité dans l'Union européenne et préviennent le terrorisme. On constate donc que le principal objectif fixé pour justifier la création d'un SSFT propre à l'UE peut être atteint par un système qui existe déjà: l'accord TFTP UE-États-Unis. Au regard de ces développements et au stade actuel, la Commission n'estime donc pas justifié d'instaurer un nouveau système de surveillance du financement du terrorisme, assorti de toutes les implications précédemment exposées, telles que l'intensification de la collecte des données à caractère personnel et le surcoût induit par sa création et sa maintenance.