COMMISSION
EUROPÉENNE

Bruxelles, le 27.11.2013
COM(2013) 842 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Un système européen de surveillance du financement du terrorisme (SSFT de l'UE)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

Un système européen de surveillance du financement du terrorisme (SSFT de l'UE)

Pour faire suite à sa communication du 13 juillet 2011 [COM (2011)429], la Commission souhaite, par la présente communication, informer le Parlement européen et le Conseil des résultats de l'étude de faisabilité portant sur la création d'un système européen de surveillance du financement du terrorisme (SSFT de l'UE).

1. CONTEXTE

1.1. Origine de la demande et définition

Lors des négociations préalables à la conclusion de l'accord TFTP entre l'Union européenne et les États-Unis[1], les parties avaient débattu des modalités les mieux à même de protéger les données à caractère personnel et de respecter les droits fondamentaux dans le cadre de cet accord. D'aucuns soutenaient que l'extraction de données sur le sol européen limiterait le volume des données transférées aux États-Unis et que le niveau des garanties en matière de protection des données s'en trouverait accru. Certains États membres voyaient une valeur ajoutée dans la mise en place, à plus long terme, d'un système européen indépendant destiné à la surveillance du financement du terrorisme. Le Parlement européen a demandé au Conseil et à la Commission de prendre toutes les mesures nécessaires pour élaborer une solution durable, juridiquement solide et européenne au problème de l'extraction des données souhaitées sur le territoire européen. Lorsqu'ils ont consenti à la conclusion du TFTP entre l'Union européenne et les États-Unis, le Conseil et le Parlement européen ont invité la Commission à leur soumettre, au plus tard un an à compter de la date d'entrée en vigueur de l'accord, un cadre juridique et technique pour l'extraction de données sur le territoire de l'Union et, dans les trois ans suivant la date d'entrée en vigueur dudit accord, de leur présenter un rapport sur l'état d'avancement de la création d'un système équivalent propre à l'Union européenne[2]. En outre, l'article 11 de l'accord TFTP entre l'Union européenne et les États-Unis prévoit que, pendant la durée de validité de cet accord, la Commission européenne réalisera une étude au sujet de l'éventuelle introduction d'un système équivalent propre à l'Union européenne permettant un transfert plus ciblé de données.

[1] JO L 195 du 27.7.2010, p. 5.
[2] Décision du Conseil du 13 juillet 2010, JO L 195 du 27.7.2010, p. 3.

Aux fins de la présente communication, il convient de distinguer un système équivalent propre à l'Union d'un cadre pour l'extraction de données sur le territoire de l'UE. Par *cadre pour l'extraction de données* sur le territoire de l'UE, on entend un système permettant d'effectuer, sur le territoire de celle-ci, des recherches sur les données que l'Union européenne transmet actuellement aux États-Unis. À l'inverse, *un système équivalent propre à l'UE* serait un système européen indépendant de surveillance du financement du terrorisme, qui consisterait à avoir accès aux données du ou des fournisseur(s) désigné(s), à y effectuer des recherches et à les analyser. La mise en place d'un système propre à l'Union européenne, quel qu'il soit, nécessiterait de modifier l'accord TFTP que celle-ci a conclu avec les États-Unis.

1.2. Mesures prises

En décembre 2010, la Commission a commandé *une étude* dont l'objet a été étendu en juillet 2011 afin d'y ajouter l'option d'instaurer un régime de conservation et d'extraction. Au cours de cette étude, la Commission a tenu quatre réunions d'experts associant des parties prenantes comme Europol, le contrôleur européen de la protection des données, le fournisseur désigné mentionné dans l'accord TFTP[3] et de nombreux experts des États membres qui représentaient les ministères intéressés, les services répressifs et du renseignement ainsi que des autorités chargées de la protection des données.

Le 13 juillet 2011, dans sa *communication au Parlement européen et au Conseil (ci-après dénommée «communication de 2011»)*, la Commission présentait cinq options envisageables qu'elle avait retenues en vue de la création d'un système européen de surveillance du financement du terrorisme («SSFT de l'UE»). Parmi ces cinq options, trois ont été jugées réalisables. En publiant cette communication de 2011, la Commission entendait susciter un débat sur la voie à suivre et alimenter l'analyse d'impact qui devait être effectuée.

Au mois d'octobre 2011, le dossier a été présenté au Conseil JAI et à la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen.

Les États membres et le Parlement européen n'ayant manifesté aucune préférence nette pour l'une ou l'autre de ces options, la Commission a décidé de toutes les passer en revue dans son

[3] Il s'agit de la Society for Worldwide Interbank Financial Telecommunication (SWIFT)

analyse d'impact et de les détailler en développant différentes sous-options. La présente communication repose sur cette analyse d'impact[4].

2. PRINCIPES ESSENTIELS AYANT GUIDE LA COMMISSION ET OPTIONS RETENUES

2.1. Les principes de la stratégie de gestion de l'information adoptés dans le cadre de la présidence suédoise

Dans son analyse de la ligne d'action proposée, la Commission prend en compte les principes essentiels définis dans la stratégie de gestion de l'information de 2009[5], qu'elle a ultérieurement intégrés puis affinés dans ses communications de 2010 sur la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice[6], et de 2012 sur le modèle européen d'échange d'informations[7].

Sont primordiaux à cet égard les principes de protection des droits fondamentaux, de nécessité, de proportionnalité et du rapport coût-efficacité.

Lorsqu'elle élabore de nouvelles propositions qui impliqueront le traitement de données à caractère personnel dans le domaine de la sécurité intérieure, la Commission a pour préoccupation première la protection des *droits fondamentaux* consacrés dans la Charte des droits fondamentaux de l'Union européenne, notamment le droit au respect de la vie privée et la protection des données à caractère personnel. Les articles 7 et 8 de la charte consacrent, en effet, le droit de toute personne «au respect de sa vie privée et familiale» et «à la protection des données à caractère personnel la concernant». L'article 16 du traité sur le fonctionnement de l'Union européenne, qui lie les États membres, les institutions, organes et organismes de l'Union, réaffirme le droit de toute personne à «la protection des données à caractère personnel la concernant». Conformément à l'article 52 de la charte, dans le respect du principe de proportionnalité, des limitations de l'exercice des droits et libertés reconnus par la Charte ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

[4] SWD 2013 (xx) du
[5] Conclusions du Conseil du 30 novembre 2009 sur une stratégie de gestion de l'information pour la sécurité intérieure de l'UE 16637/09
[6] COM(2010) 385 du 20 juillet 2010
[7] COM(2012) 735 du 7 décembre 2012

L'ingérence dans le droit au respect de la vie privée est considérée comme *nécessaire* si elle répond à un besoin impérieux, si elle est proportionnée au but poursuivi et si les motifs invoqués par les autorités publiques pour la justifier apparaissent pertinents et suffisants.

Bien qu'il soit difficile de chiffrer tous les coûts du terrorisme, le principe du *rapport coût/efficacité* demeure. Une approche *efficace par rapport à son coût* se fonde sur les solutions préexistantes afin de réduire les chevauchements au minimum et de maximiser les synergies éventuelles. Il convient d'établir si un meilleur usage des instruments existants permettrait d'atteindre les objectifs des propositions.

2.2. Angle d'approche

À la lumière des principes rappelés ci-dessus, la Commission a examiné si, par rapport à la situation actuelle, un SSFT de l'UE serait nécessaire et proportionné au regard de ses coûts, de ses avantages et de son incidence sur les droits fondamentaux.

Du point de vue des *avantages*, un système propre à l'UE pourrait accroître les capacités d'accès de l'UE et de ses États membres aux données pertinentes et renforcer leurs capacités d'analyse pour surveiller et identifier les terroristes grâce à leurs transactions financières. Puisque des transactions de cette nature peuvent fournir de précieux renseignements, que l'on peut ne pas obtenir auprès d'autres sources, cet outil aurait une valeur particulière pour la détection des activités terroristes et des acteurs impliqués. Un SSFT de l'UE pourrait, dès lors, constituer un outil complémentaire de renseignement et d'enquête dans la lutte contre le terrorisme et dans le renforcement de la sécurité au sein de l'Union européenne, en particulier si un tel système comprenait une multiplicité de fournisseurs de données financières et de types de transactions. Les avantages d'un SSFT de l'UE doivent, néanmoins, être mis en balance avec les coûts estimés de son instauration et de sa maintenance, notamment la charge financière pour l'UE, les États membres et les fournisseurs désignés des données en question.

2.3. Présentation des options

La Commission a examiné un certain nombre d'options tant pour *le cadre pour l'extraction de* données sur le territoire de l'Union que pour *le système équivalent propre à l'UE*.

2.3.1. Un cadre pour l'extraction de données sur le territoire de l'Union

Un cadre pour l'extraction de données sur le territoire de l'Union pourrait être instauré au moyen d'un système de conservation et d'extraction des données détenues par le fournisseur

désigné, en permettant l'accès direct aux données qui sont actuellement transmises aux États-Unis au titre du TFTP. Cet accès direct serait accordé aux analystes ou experts américains mandatés à cette fin.

Dans le cadre de cette option, une possibilité consisterait à conserver les données pendant un certain temps sur le serveur du fournisseur désigné et à interroger directement ce serveur. Toutefois, l'actuel fournisseur désigné mentionné dans l'accord TFTP UE-États-Unis a institué de solides mesures de sécurité et de protection des données qui ne permettent pas l'identification des personnes mentionnées dans le contenu des données du message, de sorte que son actuelle base de données ne permet pas d'effectuer des recherches à partir de données à caractère personnel. Il faudrait donc créer une base de données distincte.

Une autre solution consisterait à extraire les données et à les conserver en un autre lieu sécurisé de l'UE. Les analystes ou experts américains autorisés à effectuer les recherches pourraient se trouver physiquement dans les locaux du fournisseur désigné ou avoir accès à distance aux données. Dans tous les cas, et quel que soit l'emplacement des données, il faudrait édicter des garanties étendues et solides, adaptées à la configuration particulière du système.

2.3.2. Un système équivalent propre à l'UE

Une série d'options en faveur d'un système équivalent propre à l'UE (dont les grandes lignes sont exposées dans la communication de 2011) ont été examinées, parmi lesquelles un système entièrement centralisé au niveau de l'UE, un système décentralisé au niveau des États membres et trois systèmes hybrides dans lesquels l'Union européenne et les États membres joueraient chacun un rôle.

Chaque option recouvre différentes possibilités quant à la portée du système de l'UE. Des choix s'imposent quant aux types de messages et aux fournisseurs désignés qui seraient inclus. Un système équivalent propre à l'UE pourrait maintenir le type de messages financiers et le fournisseur désigné actuellement prévus par l'accord TFTP UE-États-Unis, ou aller au-delà.

- L'option d'un système totalement centralisé au niveau de l'Union impliquerait qu'un organisme européen unique exercerait l'ensemble des fonctions principales du système, à savoir: demander l'extraction de données, stocker les données, effectuer des

recherches dans celles-ci, procéder à l'analyse des renseignements, protéger et surveiller le système et diffuser les renseignements aux États membres. Cette option est juridiquement bancale car elle ne respecterait pas l'article 72 du TFUE, qui confirme que la responsabilité première du maintien de l'ordre public et de la sauvegarde de la sécurité intérieure incombe aux États membres. Un tel système ne serait ni réalisable, ni acceptable pour les États membres, car il nécessiterait la création d'une sorte de structure de renseignement centralisée au niveau de l'UE.

- Un système totalement décentralisé au niveau des États membres supposerait qu'il soit géré par les autorités compétentes des États membres, l'Union n'exerçant aucune fonction. Dès lors, les données pourraient être transférées vers les 28 États membres et interrogées par chacun d'eux. Cette option multiplierait les flux de données et aurait d'importantes incidences financières. Elle augmenterait également le risque que des données soient traitées de façon incohérente et que soient créés des mécanismes disparates de protection des données. En conséquence, cette option n'est pas non plus jugée viable.

Ces deux options ont donc été exclues d'une analyse plus détaillée.

Les trois options restantes pour créer un système équivalent propre à l'UE supposent de répartir les différentes fonctions entre différentes organisations aux niveaux national et de l'UE («systèmes hybrides»).

Dans chacun de ces systèmes hybrides, les données devraient être demandées de façon continue et répétée auprès du ou des fournisseurs désignés, extraites et stockées dans une base de données installée en un lieu sécurisé dans l'UE. Les recherches proprement dites seraient alors lancées dans cette base de données centrale. De la même façon, pour toutes les options, il conviendrait de mettre en place des garanties adaptées en matière de protection des données.

- A) Dans le premier système hybride, le service de coordination et d'analyse du SSFT de l'UE, il faudrait créer une unité centrale de l'Union. Cette unité serait chargée d'adresser les demandes de données au(x) fournisseur(s) désigné(s), d'effectuer les recherches, d'analyser les renseignements et de diffuser les résultats de ces analyses. La différence par rapport à un système entièrement centralisé résiderait dans le fait que les États membres auraient un accès direct au système et pourraient demander que des

recherches soient effectuées en leur nom par l'unité centrale ou par leurs propres analystes.

- B) Le deuxième système hybride, le service d'extraction du SSFT de l'UE, impliquerait également la création d'une unité centrale de l'Union. Toutefois, dans le cadre de cette option, l'organisme de l'UE effectuerait les recherches à la demande des États membres et leur en transmettrait les résultats sans analyser les informations obtenues. Il pourrait toutefois lancer ses propres recherches et en analyser le résultat.

- C) Dans le dernier système hybride, dénommé service de coordination des cellules de renseignement financier («CRF»)[8], une structure européenne ad hoc serait créée. Il s'agirait non pas d'un organisme permanent mais plutôt d'un groupe d'experts en renseignement financier qui se réuniraient. La plate-forme des CRF pourrait, à cette fin, être modernisée. Chaque État membre désignerait un représentant qui agirait en son nom. Cette instance ad hoc recueillerait les demandes de la CRF de chaque État membre et adresserait les demandes de données que le ou les fournisseurs désignés devraient fournir à la suite des demandes des États membres. Le représentant de chaque État membre serait chargé d'effectuer les recherches, de procéder aux analyses et de gérer les résultats au nom de son propre État membre. Il appartiendrait ensuite aux autorités compétentes des États membres d'exploiter les renseignements obtenus et de les diffuser au niveau national.

2.3.3. Statu quo: l'accord TFTP entre l'Union européenne et les États-Unis

À l'heure actuelle, l'Union et les États membres peuvent demander que des recherches soient effectuées par les États-Unis au titre de l'accord TFTP UE-États-Unis, lequel régit 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 («TFTP»).

Le TFTP est un outil antiterroriste que les États-Unis ont conçu au lendemain des attentats terroristes du 11 septembre. Il consiste à effectuer des recherches sur des données transmises par le fournisseur désigné, y compris celles transférées de l'Union européenne.

[8] Décision du Conseil du 17 octobre 2000 relative aux modalités de coopération entre les cellules de renseignement financier des États membres en ce qui concerne l'échange d'informations

L’accord TFTP UE-États-Unis réglemente minutieusement la procédure de demande de données par les autorités américaines. Europol vérifie que ces demandes reçues des États-Unis sont conformes à l’accord et, en particulier, qu’elles sont adaptées aussi strictement que possible afin de réduire au minimum le volume des données qui seront transférées. De nombreuses dispositions régissent le traitement, le stockage et l'effacement sécurisés des données. Les données fournies sont conservées dans un environnement sécurisé et stockées séparément de toutes les autres données. L’accord prévoit une durée de conservation de cinq ans et une obligation d’évaluer régulièrement la nécessité de conserver les données. Parmi les contrôleurs indépendants établis aux États-Unis figurent deux contrôleurs sélectionnés par l’Union européenne. Les contrôleurs exercent un contrôle continu sur le mode de fonctionnement du système et ont la faculté de vérifier chaque recherche menée par le département du Trésor des États-Unis, pour s'assurer que l’objet de la recherche a un lien avec le terrorisme ou son financement.

L’accord comporte également des dispositions sur le droit d’accès aux données à caractère personnel et le droit de rectification de celles-ci, ainsi que sur les procédures de recours. Selon l'accord, toute personne estimant que des données à caractère personnel la concernant ont fait l'objet d'un traitement en violation de l'accord dispose d'un droit de recours administratif ou judiciaire effectif en application de la législation de l'Union européenne, de ses États membres et des États-Unis, respectivement. L'accord prévoit que toute personne, indépendamment de sa nationalité ou de son pays de résidence, a accès, en vertu du droit des États-Unis, à une procédure lui permettant d’introduire un recours en justice contre un acte administratif défavorable.

Parmi les lois applicables à l'exercice d'un recours en justice contre un acte administratif défavorable adopté par le département du Trésor, en rapport avec des données à caractère personnel reçues en application de l’accord, figurent la loi sur les procédures administratives (Administrative Procedure Act) et la loi sur la liberté de l’information (Freedom of Information Act). La loi sur les procédures administratives permet aux personnes ayant subi un préjudice du fait d'un acte imputable au gouvernement des États-Unis de solliciter le contrôle juridictionnel de cet acte. La loi sur la liberté de l’information, quant à elle, permet aux personnes d’utiliser les recours administratifs et judiciaires pour solliciter des archives du gouvernement. Les actuelles procédures uniformes d’accès aux données à caractère personnel,

et/ou de rectification, d'effacement ou de verrouillage de celles-ci, convenues entre la Commission, les États-Unis et le groupe de travail «article 29», visent à faciliter l'exercice de ces droits par les citoyens de l'Union. La mise en œuvre de l'accord ainsi que les garanties et contrôles qu'il prévoit sont réexaminés régulièrement en application de son article 13. Deux de ces réexamens ont été effectués en 2011[9] et 2012[10], dont il est ressorti que l'accord avait été correctement mis en œuvre. Un troisième réexamen est prévu pour le printemps 2014. Le rapport conjoint relatif à la valeur des données fournies, préparé conformément à l'article 6 de l'accord, démontre l'effet bénéfique du TFTP en matière de prévention et de répression du terrorisme et de son financement , et l'utilisation que plusieurs États membres font ou ont fait de ce programme. Grâce à leur exactitude et leur précision, les informations du TFTP permettent d'identifier et de surveiller les terroristes et leurs réseaux de soutien à travers le monde. Elles fournissent des indications sur les structures financières actuelles des organisations terroristes et elles permettent de repérer de nouvelles filières de financement et d'identifier les acteurs en cause.

3. ÉVALUATION

Lorsqu'elle apprécie l'opportunité de proposer la création d'un SSFT de l'UE, la Commission doit concilier les différents points de vue et attentes concernant le niveau d'ambition d'un système européen. Les multiples décideurs et parties prenantes ont, en effet, chacun leur opinion sur les objectifs que doit poursuivre un tel système. La Commission a examiné les possibilités et les conséquences des deux scénarios à l'aune des principes à respecter lors de l'élaboration et de la mise en œuvre de nouvelles initiatives, détaillés plus haut. Concrètement, chaque option a été soupesée du point de vue de la nécessité, de la proportionnalité et du rapport coût/efficacité.

3.1. Un cadre pour l'extraction de données sur le territoire de l'UE

Décrite au point 2.3.1, cette option prévoyant un régime de conservation et d'extraction des données constituerait un moyen de collecter, de stocker et de consulter sur le territoire de l'Union les données qui sont actuellement transférées aux États-Unis au titre de l'accord TFTP UE-États-Unis. Elle ne permettrait donc pas à l'UE ou aux États membres d'obtenir davantage de renseignements par rapport à la situation actuelle. Au contraire, les données TFTP étant

[9] SEC(2011) 438 du 30 mars 2011.
[10] SWD(2012) 454 du 14 décembre 2012.

stockées à la fois aux États-Unis et dans l'UE, la fragmentation des recherches, qui se font actuellement sur un seul ensemble de données TFTP, risquerait d'avoir une incidence négative sur la qualité et le nombre des renseignements et de compromettre l'efficacité globale du TFTP. Elle pourrait aussi ralentir sensiblement le processus d'analyse, puisque plusieurs recherches consécutives dans les données TFTP stockées en deux endroits différents pourraient être nécessaires pour exploiter un renseignement. Or la rapidité est souvent essentielle lorsque l'on enquête sur le terrorisme.

L'extraction des données réalisée sur le territoire européen, au lieu des États-Unis, ne garantirait pas, en soi, une meilleure protection des données à caractère personnel. Il est capital de protéger l'accès aux données pour les gérer correctement, quel que soit le lieu. À cette fin, un ensemble de garanties solides devrait être mis en place pour assurer la conformité du traitement et de la gestion des données avec les exigences nécessaires. Le système devrait être pourvu d'une fonction de contrôle pour vérifier les demandes de recherche et leur justification. Le rôle des contrôleurs indépendants serait déterminant pour garantir que les données soient utilisées aux seules fins définies dans l'accord instituant le système. Des mesures devraient être prises pour prévenir l'accès non autorisé aux données ou leur divulgation, par exemple en les conservant dans un environnement sécurisé. Des procédures régissant l'accès aux données à caractère personnel et leur rectification, ainsi que des moyens de recours appropriés, devraient être intégrés. Un audit externe devrait être commandé pour vérifier le bon fonctionnement du système.

Dans le cadre de l'accord TFTP UE-États-Unis, les autorités américaines n'ont pas accès à la totalité des données du fournisseur désigné, mais uniquement aux ensembles de données qu'elles ont demandés et qu'Europol a approuvés, compte tenu des analyses du risque terroriste passé et présent. À moins de mettre en place un mécanisme similaire de réduction initiale des demandes de données, autoriser des recherches directes sur la totalité des données du fournisseur désigné multiplieraient encore les risques pour ces dernières et les incidences sur le droit à la protection des données. Cela exigerait du fournisseur désigné une réorganisation considérable de son fonctionnement et de son mode de stockage des données. En effet, à l'heure actuelle, les messages financiers qui relèvent de l'accord sont conservés sous une forme qui ne permet pas d'identifier les personnes mentionnées dans le contenu des données du message. Chaque message financier est crypté et ne peut être recherché qu'à l'aide.

des métadonnées, à savoir la date d'envoi du message, le type de message et les banques émettrice et destinataire concernées. Le fournisseur désigné a ainsi mis en place de solides mesures de sécurité et de protection des données afin de protéger les données de ses clients du monde entier. Dès lors, pour permettre d'effectuer des recherches directement sur le serveur actuel du fournisseur désigné, il faudrait d'abord décrypter tous ces messages. Or cette opération serait excessive et disproportionnée car ce serveur contient davantage de messages qu'il n'est nécessaire pour lutter contre le financement du terrorisme. En outre, un accès direct à des fins de recherche serait extrêmement dérangeant pour les activités courantes du fournisseur désigné et créerait des risques non négligeables pour le fonctionnement, la sécurité et le système. Cette option rendrait donc nécessaire la création d'une base de données distincte sur le territoire de l'UE pour y détenir les informations nécessaires du fournisseur désigné.

Des investissements importants seraient indispensables pour mettre le système en place et garantir sa pleine conformité avec les règles de sécurité. Les locaux du fournisseur désigné ou un autre lieu sécurisé devraient être adaptés aux besoins spécifiques, des solutions informatiques et techniques devraient être mises au point et appliquées, et du personnel hautement qualifié devrait être recruté et formé pour gérer et superviser ce système.

En retenant cette option, l'UE et les États membres assumeraient tous les inconvénients et les coûts d'un mécanisme créé uniquement pour le TFTP, qui est un instrument appartenant à un pays tiers. Dans le contexte actuel, cette option n'apparaît ni nécessaire ni proportionnée ni d'un bon rapport coût/efficacité, car elle ne permettrait pas d'obtenir davantage de renseignements, elle serait coûteuse et difficile à mettre en place et elle pourrait engendrer des risques pour la protection des données à caractère personnel.

3.2. Un système équivalent propre à l'UE

Aucune évaluation plus détaillée n'a été réalisée au sujet d'un SSFT de l'UE entièrement centralisé, en raison de l'absence de base juridique et de la faible probabilité que les États membres acceptent de confier à l'UE un rôle centralisateur dans un domaine qui relève de leur compétence nationale. Un tel système a été exclu parce qu'il entraînerait des coûts considérables et de multiples incidences sur le droit à la protection des données. Les trois systèmes hybrides évalués permettraient aux États membres d'exercer un contrôle, à des

degrés variables, sur les recherches effectuées par les autres États membres et par l'organisme de l'UE centralisé.

Élargir la portée d'un système équivalent propre à l'UE pour y englober les chambres de compensation informatisées, la monnaie électronique et d'autres données non financières permettrait d'obtenir davantage de renseignements, la capacité de l'Union de surveiller les paiements effectués sur son territoire étant accrue, et de créer un système qui résisterait mieux à l'épreuve du temps qu'un système ne traitant que des messages financiers. Cependant, chaque addition d'un fournisseur désigné augmenterait le risque de violation du droit à la protection des données et requerrait donc un ensemble de conditions, de garanties et de mesures de contrôle rigoureuses. La charge administrative pesant sur les fournisseurs désignés s'en trouverait également augmentée. Ajouter de multiples fournisseurs de données et de nombreux messages pour créer un système aussi complexe et aussi lourd du point de vue organisationnel et technique accroîtrait, en outre, substantiellement les coûts.

Cette analyse conduit à conclure que tout SSFT de l'UE qui pourrait voir le jour n'utiliserait que les données des messages, la Commission estimant que les avantages supplémentaires apportés par le recours à de multiples fournisseurs et types de données ne compensent pas le coût considérable à la charge des entreprises privées ni les atteintes à la vie privée et au droit à la protection des données qu'un tel système impliquerait. Ainsi, puisque le système de l'UE comprendrait exclusivement le même fournisseur désigné et le même type de messages que le TFTP, la qualité et la quantité de renseignements reçus, ainsi que les risques pour les données, seraient comparables à ceux du TFTP UE-États-Unis.

Comme il a été expliqué ci-dessus, il existe trois options pour ce système équivalent propre à l'UE: A) le service de coordination et d'analyse SSFT de l'UE, B) le service d'extraction SSFT de l'UE et C) le service de coordination des CRF.

L'option A serait susceptible d'avoir un effet bénéfique sur la prévention du terrorisme et le renforcement de la sécurité dans l'UE. En effet, si l'on confie les recherches et l'analyse des résultats aux équipes de l'Union et à celles des États membres, les exigences en matière de renseignements fixées par l'UE et par les États membres seront pleinement prises en compte et le système sera axé sur la «menace contre l'UE». Ce progrès dépendra toutefois d'une volonté et d'une capacité accrues des États membres d'échanger des informations et des

analyses, à moyen et à long terme. Il est difficile de prédire dans quelle mesure on pourra compter sur cette augmentation des flux d'informations. En outre, comme les États membres conserveraient la faculté de demander que des recherches soient effectuées à partir des États-Unis, au titre du TFTP, ce système exigerait une forte adhésion et une étroite coopération de la part des États membres s'il était censé donner une image plus cohérente de la situation dans l'UE.

L'option B pourrait avoir certains effets positifs sur la prévention du terrorisme et le renforcement de la sécurité dans l'UE. Le système permettrait de mieux donner suite aux analyses des menaces pesant sur l'UE car les recherches seraient effectuées en fonction des besoins de renseignements des États membres. Le rôle de l'organisme de l'UE centralisé se limiterait toutefois à effectuer des recherches et à transférer les données obtenues à l'État membre requérant; il ferait ainsi davantage office de contrôleur d'accès qu'autre chose. Dès lors, aucune analyse ne serait réalisée au niveau de l'UE et le système ne fonctionnerait que si les États membres échangeaient des analyses, en dehors du système, si l'on voulait dresser un état cohérent du renseignement dans l'UE. Le système ne pouvant garantir que les recherches soient définies uniformément, il augmenterait le risque de faux positifs et, de ce fait, porterait atteinte à la protection des données et de la vie privée.

L'option C répondrait aux besoins de renseignements propres à chaque État membre et aurait ainsi certains effets bénéfiques sur la prévention du terrorisme et le renforcement de la sécurité. Toutefois, comme les CRF nationales seraient chargées des recherches et des analyses de leur État membre, cette option présente les mêmes inconvénients que l'option B — on n'obtiendrait une véritable vue d'ensemble que moyennant une coopération renforcée entre les États membres, en dehors du système. De plus, les CRF ciblent uniquement le renseignement financier, et le clivage entre ce type d'informations et le panorama plus large du renseignement pourrait accroître la difficulté de percevoir les liens et de repérer le financement du terrorisme. Cette option pèche également par la très faible participation de l'UE; les capacités seraient renforcées en premier lieu au niveau national.

Toutes ces options auraient un coût important pour l'UE, pour les États membres et pour le fournisseur désigné, notamment, entre autres, le coût de mise au point de l'infrastructure informatique, les installations sécurisées et le coût des dizaines, voire centaines, d'agents chargés de gérer le système et de mettre en œuvre les garanties et les contrôles. Néanmoins,

chacun de ces systèmes envisageables est en mesure de contribuer à une meilleure sécurité européenne car ils reposeraient tous sur des évaluations de la menace correspondant aux besoins de l'UE.

Un outil de renseignement et de recherche indépendant installé sur le territoire européen supprimerait l'obligation de transférer les données vers les États-Unis. Mais tout SSFT de l'UE requerrait encore des garanties et contrôles étendus en matière de protection des données, analogues à ceux déjà en vigueur dans le cadre de l'accord TFTP UE-États-Unis et, en tout état de cause, le respect de l'acquis de l'UE et des États membres en cette matière. Pour toute demande de recherches parmi des données stockées dans les systèmes de l'UE, il devrait être vérifié si la stricte limitation à la finalité de la lutte contre le terrorisme et son financement est respectée, y compris la question de savoir si le transfert de données est justifié. Concrètement, des contrôleurs indépendants qualifiés devraient s'assurer que chaque recherche de l'UE et de chaque État membre a été dûment autorisée et était nécessaire à la lutte contre le terrorisme et son financement. La gestion et le stockage sécurisés des données devraient être assurés, et l'accès non autorisé aux données, évité. Un audit externe du bon fonctionnement du système et de l'ensemble de ses garanties serait nécessaire. Toutes les procédures requises pour avoir accès aux données à caractère personnel et rectifier ces dernières, ainsi que des moyens de recours appropriés, devraient être intégrés dans le système.

En conclusion, conformément aux demandes formulées par le Parlement européen et le Conseil, la Commission a examiné les options envisageables pour la création d'un SSFT de l'UE, dont un régime d'extraction et de conservation.

Cette évaluation prend en considération les principes consacrés dans la stratégie de gestion de l'information qui avait été adoptée sous la présidence suédoise. Tout système mis en place doit être nécessaire, proportionné et d'un bon rapport coût/efficacité, et doit respecter les droits fondamentaux. Ainsi qu'il est explicité ci-dessus et dans l'analyse d'impact, l'analyse réalisée par la Commission indique que chacune des options réalisables présente des avantages et des inconvénients. En revanche, la Commission a écarté les options qui ne sont pas réalisables, comme il est expliqué plus haut.

À la lumière des informations recueillies, peu d'arguments plaident, à ce stade, en faveur de la présentation d'une proposition portant création d'un SSFT de l’UE.

La Commission invite le Parlement européen et le Conseil à formuler leurs observations sur la présente communication.