CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 15 juillet 2011 (18.07)
(OR. en)

12957/11

GENVAL 81
JAI 522
ECOFIN 523
DATAPROTECT 75
ENFOPOL 245

NOTE DE TRANSMISSION

Origine:	Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur
Date de réception:	14 juillet 2011
Destinataire:	Monsieur Uwe CORSEPIUS, Secrétaire général du Conseil de l'Union européenne
N° doc. Cion:	COM(2011) 429 final
Objet:	**COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU CONSEIL ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme**

Les délégations trouveront ci-joint le document de la Commission - COM(2011) 429 final.

p.j.: COM(2011) 429 final

COMMISSION EUROPÉENNE

Bruxelles, le 13.7.2011
COM(2011) 429 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU CONSEIL ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS

Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU CONSEIL ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS

Options envisageables pour la création d'un système européen de surveillance du financement du terrorisme

1. INTRODUCTION

Lorsque le Conseil a consenti à la conclusion d'un 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 (ci-après, l'«accord TFTP UE-USA»)[1], il a également invité la Commission à soumettre au Parlement européen et au Conseil, au plus tard un an après la date d'entrée en vigueur de l'accord (le 1er août 2010), «un cadre légal et technique pour l'extraction des données sur le territoire européen»[2]. De même, le Parlement européen a demandé à plusieurs reprises qu'à plus long terme, une solution durable, juridiquement solide et européenne au problème de l'extraction des données souhaitées sur le territoire européen soit envisagée[3]. La communication intitulée «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre» indiquait déjà que la Commission élaborerait, en 2011, une politique relative à l'extraction et à l'analyse des données de messagerie financière détenues sur son territoire[4]. Vu l'efficacité avérée du TFTP américain, le futur système européen devrait contribuer grandement aux efforts déployés pour couper l'accès des terroristes aux sources de financement et aux substances CBRN, et suivre leurs transactions. On peut également mentionner l'article 11 de l'accord TFTP UE-USA, qui 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. La présente communication est le premier volet de la réponse apportée par la Commission audit article et à l'invitation du Conseil. Elle décrit les différentes démarches entreprises par la Commission pour avancer sur la voie de l'instauration d'un tel «cadre légal et technique» et présente les diverses options examinées pour atteindre cet objectif. Elle n'indique pas à ce stade l'option privilégiée, mais elle expose les points pertinents à prendre en considération pour chacune des options envisagées. Vu l'importance politique de la question examinée et sa complexité juridique et technique, la Commission tient à informer le Conseil et le Parlement de l'état d'avancement du dossier et à susciter un débat. Elle estime que ce nouveau débat sera utile avant de proposer, sur la base d'une analyse d'impact, des mesures concrètes.

Dans ce contexte, il convient de souligner que la présente communication ne préjuge pas de la future proposition de la Commission, qui tiendra compte des discussions susmentionnées et de l'analyse d'impact, laquelle sera fondée sur une étude que la Commission a commandée au cours du second semestre de 2010. Vu l'incidence qu'une proposition législative aurait sur les

---

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.

3 Voir, par exemple, la résolution P7_TA(2010)0143 et l'exposé des motifs de la recommandation A7-0224/2010.

4 COM(2010) 673 final du 22.11.2010. Voir l'action 2 relevant de l'objectif 2, p. 8.

droits fondamentaux et, notamment, sur la protection des données, l'analyse d'impact s'attachera en particulier à déterminer si les mesures proposées par la Commission respectent les critères de nécessité et de proportionnalité. À cette fin, la Commission suivra les orientations énoncées dans sa communication relative à la stratégie pour la mise en œuvre effective de la charte des droits fondamentaux[5].

En outre, l'analyse d'impact fournira les données techniques de référence nécessaires, ainsi qu'une évaluation détaillée de toutes les options envisagées. Ces questions ont déjà été examinées avec de nombreuses parties intéressées dans le domaine concerné, y compris des autorités nationales, des autorités chargées de la protection des données, Europol et le prestataire désigné. Les résultats définitifs de l'étude précitée ne seront disponibles qu'à la fin de l'année. Afin de préparer l'analyse d'impact, la Commission européenne a organisé trois réunions d'experts, rassemblant les mêmes parties prenantes, ainsi que les autorités américaines chargées de la gestion du TFTP. Les options envisagées dans la présente communication s'appuient sur les résultats préliminaires de l'étude et sur les débats qui sont intervenus lors de ces réunions d'experts.

2. OBJECTIFS DE LA CREATION D'UN SYSTEME EUROPEEN DE SURVEILLANCE DU FINANCEMENT DU TERRORISME

La création d'un système de surveillance du financement du terrorisme (SSFT) propre à l'UE se justifie doublement:

- le système contribuera efficacement à la lutte contre le terrorisme et contre son financement dans l'Union européenne;

- il contribuera à limiter le volume de données à caractère personnel qui sont transférées vers des pays tiers. Il devrait permettre le traitement des données nécessaires à son fonctionnement sur le territoire de l'Union, dans le respect des principes et de la législation de l'UE en matière de protection des données.

Aux États-Unis, le programme de surveillance du financement du terrorisme (TFTP) s'est révélé porteur d'une importante valeur ajoutée pour la lutte contre le terrorisme et son financement, qui profite non seulement aux autorités américaines mais aussi à celles des États membres de l'Union et des pays tiers. Le réexamen récent de l'accord TFTP UE-USA[6] a confirmé que depuis la mise en place du TFTP aux États-Unis, plus de 2 500 rapports ont été communiqués aux autorités de pays tiers, dont l'écrasante majorité (1 700) a été partagée avec l'Union européenne. Le juge Bruguière, que la Commission européenne a nommé en 2008 pour procéder à ce réexamen, a confirmé l'efficacité du programme américain et la précieuse contribution qu'il apporte à la lutte contre le terrorisme et son financement. Parmi les données recueillies dans le cadre du TFTP transmises aux autorités de l'UE figuraient des indices importants liés à plusieurs actes terroristes ou tentatives d'attentat de premier plan, et notamment: les attentats de Madrid et Londres, le complot de 2006 visant à détruire des avions assurant des liaisons transatlantiques à l'aide d'explosifs liquides, ainsi que la tentative déjouée d'attaque contre des intérêts américains en Allemagne en 2007. L'équipe de l'UE chargée du réexamen a également conclu qu'elle avait reçu des «preuves convaincantes de la

---

5 COM(2010) 573 final du 19.10.2010.

6 SEC(2011) 438 final du 30.3.2011.

contribution du TFTP aux efforts de lutte contre le terrorisme et son financement». Compte tenu de ces éléments, il y a tout lieu de croire que le SSFT de l'UE contribuera grandement aux efforts déployés par l'Union et ses États membres pour combattre le terrorisme et son financement.

Si l'efficacité du TFTP américain dans ce combat n'est aucunement mise en doute, ses répercussions sur les droits fondamentaux des citoyens ont suscité de graves préoccupations. Celles-ci proviennent essentiellement du fait que l'application de l'accord TFTP UE-USA entraîne la communication d'importants volumes de données à caractère personnel («transfert de données en masse») aux autorités américaines, dont la grande majorité concerne des citoyens qui n'ont aucun rapport avec le terrorisme ou son financement. Les données sont ainsi transmises massivement (selon les catégories de données correspondantes) plutôt qu'au cas par cas (en réponse à une demande relative à une ou plusieurs personnes), car le prestataire qui fournit les données n'a pas la capacité technique de les transmettre au cas par cas. En outre, pour que le prestataire puisse communiquer ces données sur une base individuelle, il faudrait créer une fonctionnalité spéciale de recherche et d'analyse, qui n'est pas exigée par ses processus opérationnels et aurait d'importantes répercussions en termes de ressources. Par ailleurs, la transmission des données au cas par cas aurait en réalité pour effet d'informer le prestataire des noms des personnes faisant l'objet d'une recherche dans le cadre d'enquêtes sur le terrorisme et de leurs relations financières. L'efficacité de ces enquêtes pourrait ainsi s'en trouver affectée.

Afin de contrebalancer les effets du transfert massif de données, des garanties importantes ont été mises en place pour empêcher toute utilisation abusive des données, dont celle consistant à n'autoriser la consultation et l'utilisation des données du prestataire qu'aux fins de la lutte contre le terrorisme et son financement. Le réexamen récent de l'accord TFTP UE-USA a confirmé que ces garanties sont effectivement appliquées dans le respect des dispositions de l'accord.

Cependant, d'aucuns soutiennent que la transmission à un pays tiers de volumes si importants de données à caractère personnel constitue une violation injustifiée des droits fondamentaux des citoyens concernés, si l'on considère cette violation au regard des critères de nécessité et de proportionnalité. C'est pourquoi le Conseil a invité la Commission à présenter des propositions en vue de la création d'un système permettant «l'extraction de données sur le territoire de l'UE»; l'objectif général est de faire en sorte que le traitement de ces données soit effectué dans le respect de la législation et des principes de l'Union en matière de protection des données et dans le respect de la charte des droits fondamentaux de l'UE. Il convient à cet égard de noter que la collecte et le traitement de données financières par les pouvoirs publics portent atteinte au droit à la protection des données à caractère personnel, que consacrent l'article 16 du traité sur le fonctionnement de l'UE (TFUE) et l'article 8 de la charte.

Conformément à l'article 52, paragraphe 1, de la charte, toute limitation de l'exercice de ces droits fondamentaux doit être prévue par la loi, avec la précision et la qualité requises pour assurer sa prévisibilité, et respecter le contenu essentiel desdits droits. Elle doit s'en tenir à ce qui est nécessaire et proportionné pour répondre à un objectif légitime reconnu par l'Union. Il y a donc lieu de tenir compte de ces principes non seulement au moment de décider de la création d'un SSFT de l'UE, mais aussi lors de l'examen des différentes options envisageables pour mettre ce système en œuvre. Par conséquent, ces principes influencent également les choix à effectuer sur des questions telles que la portée du système, les durées de conservation applicables, les droits des personnes en matière d'accès, de suppression, etc. La présente

communication ne traite pas ces questions dans le détail, qui devront faire l'objet d'un examen minutieux dans l'analyse d'impact.

À l'évidence, la création envisagée d'un système d'extraction de données sur le territoire de l'UE aurait des répercussions sur l'accord TFTP UE-USA, comme le reconnaît l'article 11, paragraphe 3, de l'accord qui s'énonce comme suit: la mise en place d'un système de l'Union européenne étant susceptible de modifier considérablement le contexte de l'accord, il convient que les parties se consultent afin de déterminer si l'accord doit être adapté, si l'Union européenne décide de mettre en place un tel système. Toutes les options auraient donc aussi une incidence sur la mise en œuvre future de l'accord TFTP UE-USA et entraîneraient son adaptation en conséquence.

3. FONCTIONS PRINCIPALES D'UN SYSTEME EUROPEEN DE SURVEILLANCE DU FINANCEMENT DU TERRORISME

L'un des premiers points saillants des discussions avec les parties intéressées susmentionnées est que la grande majorité de celles-ci estime que si le SSFT de l'UE doit être créé, il doit l'être dans le but d'assurer la sécurité des citoyens de l'Union. Le système ne doit pas être établi à la seule fin de fournir des informations utiles aux autorités américaines: les résultats quel le système permettra d'obtenir revêtiront également un réel intérêt pour les autorités des États membres. En outre, selon cette approche, l'équivalent européen du TFTP américain ne devrait pas nécessairement en reprendre tous les éléments, même si ce dernier pourrait assurément être une source d'inspiration. Par ailleurs, le système de l'UE devait être établi en tenant compte de la spécificité du cadre juridique et administratif de l'Union, y compris du respect des droits fondamentaux concernés indiqués ci-dessus.

Cependant, tout système destiné à surveiller le financement du terrorisme en vue d'atteindre les principaux objectifs décrits ci-dessus doit prévoir la mise en œuvre des fonctions essentielles suivantes:

- préparer et envoyer, au(x) prestataire(s) désigné(s) de services de messagerie financière, les demandes (juridiquement valables) de transmission de données brutes à un ou plusieurs destinataires habilités. Cela implique de déterminer les catégories de messages à demander ainsi que la fréquence d'envoi de ces messages, et de maintenir des contacts avec les prestataires sur ces questions;

- contrôler et autoriser les demandes de données brutes adressées au(x) prestataire(s) désigné(s). Cela implique de vérifier si la demande de données brutes a été établie dans le respect des limites applicables;

- recevoir et stocker (traiter) les données brutes émanant du (des) prestataire(s) désigné(s), et notamment instaurer un système adéquat pour la sécurité des données physiques et électroniques;

- procéder aux recherches en tant que telles dans les données fournies, conformément au cadre juridique applicable, sur la base des demandes de recherche introduites par les autorités des États membres, des États-Unis ou d'autres pays tiers dans le respect de conditions et garanties clairement définies, ou à l'initiative de l'autorité ou des autorités chargée(s) du traitement des données;

- contrôler et autoriser la réalisation de recherches dans les données fournies;

- analyser les résultats des recherches, en les confrontant à d'autres informations ou éléments de renseignement disponibles;

- diffuser les résultats des recherches (sans autre analyse) ou les résultats des analyses aux destinataires habilités;

- mettre en œuvre un régime adéquat de protection des données, y compris des délais de conservation à respecter, des obligations en matière de journalisation, et traiter les demandes d'accès, de correction et de suppression, etc.

Ces fonctions essentielles devraient être définies dans des instruments juridiques appropriés au niveau de l'Union, au niveau national, ou à ces deux niveaux, selon l'option retenue.

4. PRINCIPES CLES DEVANT GUIDER L'EXAMEN DES OPTIONS ENVISAGEABLES

Outre les considérations relatives aux fonctions essentielles exposées ci-dessus, le choix entre les options possibles dépendra pour une grande part de leur examen au regard d'un certain nombre de critères déterminants, qui sont actuellement étudiés dans le cadre de l'analyse d'impact et abordés ci-dessous.

4.1. Efficacité

L'efficacité escomptée des différentes options s'agissant d'atteindre l'objectif fondamental de lutte contre le terrorisme et son financement est un élément décisif. De ce point de vue, il convient de privilégier les options qui augmentent les possibilités de partage et d'analyse des données au niveau international, car ce partage et cette analyse accroîtront l'efficacité et la valeur ajoutée obtenues. En particulier, le choix du ou des organismes qui seront chargés d'analyser les données et de communiquer les résultats de ces analyses aux autorités compétentes influencera notablement l'efficacité globale du système, ainsi que le volume des données qui seront transférées. Les États membres devraient malgré tout, conformément aux pratiques actuelles, rester pleinement libres de décider si les informations ou éléments de renseignement dont ils disposent peuvent être transmis à d'autres autorités.

4.2. Protection des données

Le partage et l'analyse d'informations et d'éléments de renseignement à l'échelle internationale ne peuvent intervenir que dans le cadre d'un régime de protection des données solide et bien développé. L'efficacité de ce régime dépend non seulement des dispositions juridiques applicables, qui permettent aux personnes concernées d'exercer leurs droits, comme le droit à un recours juridictionnel, mais aussi de la disponibilité de personnels expérimentés, tels que des responsables indépendants de la protection des données, et d'autorités compétentes chargées de contrôler la protection des données. Certains des organismes qui pourraient être associés à l'éventuelle création d'un SSFT de l'UE disposent déjà de telles structures, tandis que d'autres devraient les mettre en place. Par conséquent, il convient d'évaluer soigneusement les implications pour la protection des données que comporte chacune des options, conformément aux principes primordiaux liés au respect des droits fondamentaux visés au point 2 de la présente communication.

4.3. Sécurité des données

Il convient de combiner une réglementation solide en matière de protection des données avec des infrastructures et technologies de pointe dans le domaine de la sécurité des données. Les exigences en matière de sécurité des données plaident en faveur d'une limitation du nombre de sites où les données fournies pourraient être traitées, ainsi que d'une restriction de toutes les formes d'accès aux données depuis l'extérieur. La solution offrant la plus grande sécurité consisterait à prévoir le stockage en un seul endroit, en excluant tout accès depuis l'extérieur. La plupart des organismes susceptibles d'être associés à la gestion du SSFT disposent déjà de technologies permettant le traitement sécurisé des données, mais tous n'ont pas la capacité de traiter des données dont la classification est supérieure au niveau «Restreint UE».

4.4. Stockage des données

Le stockage des données pourrait être organisé à l'échelon national ou de l'UE. Au niveau de l'Union, les données émanant du (des) prestataire(s) désigné(s) pourraient être stockées dans les locaux d'Europol ou d'un autre organe de l'UE, comme l'Agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice (ci-après, l'«agence chargée des systèmes d'information»)[7], dont la mise en place est en cours. Le stockage des données étant inextricablement lié aux questions de protection et de sécurité des données, le choix de l'organisme qui en sera chargé dépendra fortement du régime de protection et de sécurité des données qu'il pourra offrir.

4.5. Utilisation des structures et instruments existants

Quelle que soit l'option retenue, il conviendra, autant que possible, d'avoir recours aux structures existantes. Les coûts seront ainsi limités et il sera possible de profiter de l'expérience acquise ainsi que des infrastructures en place. Cette utilisation d'instruments déjà créés implique que les nouvelles tâches qui seraient confiées à un organisme existant cadrent avec son mandat. Par exemple, Europol, Eurojust ou les autorités judiciaires nationales pourraient se voir confier les fonctions de vérification et d'autorisation des demandes de fourniture de données adressées au(x) prestataire(s) désigné(s),

4.6. Coopération entre les autorités compétentes

Les options décrites ci-dessous permettent, à des degrés variables, une coopération et un partage de l'information et du renseignement entre autorités nationales, d'une part, et entre autorités nationales et européennes, d'autre part. Différents États membres ont adopté diverses formes de coopération entre leurs autorités nationales pour lutter contre le terrorisme, et toute action entreprise au niveau européen doit respecter les limites établies par l'article 72 du TFUE relatif aux prérogatives des États membres en matière de maintien de l'ordre public et de sauvegarde de la sécurité intérieure. Le SSFT de l'UE, quel qu'il soit, devra donc permettre aux États membres de disposer d'un degré de contrôle important sur l'information et le renseignement qu'ils accepteront de partager dans le cadre de ce système. Un certain nombre d'organismes évoqués ci-dessous ont adopté différentes approches de cette question, dont certaines pourraient être directement applicables au système à établir.

---

[7] COM(2010) 93 final du 19.3.2010.

4.7. Premier aperçu général des incidences financières possibles des différentes options

Le coût global de la création d'un SSFT de l'UE et sa ventilation entre les autorités européennes et nationales dépendront en grande partie de l'option stratégique retenue. Les dépenses comprendront en tout état de cause:

- le coût du transfert et du stockage sécurisés des données émanant du (des) prestataire(s) désigné(s);
- le coût du développement et de la maintenance du logiciel nécessaire pour procéder aux recherches et fournir les résultats de celles-ci;
- le coût de la diffusion des résultats des recherches ou des analyses aux destinataires autorisés/habilités;
- le coût du personnel chargé de procéder aux recherches et analyses et d'en diffuser les résultats;
- le coût du personnel chargé des fonctions de contrôle et d'audit;
- le coût du personnel chargé de la protection des données et des droits des citoyens.

Bien qu'à ce stade on ne dispose pas encore d'estimations précises des coûts, les premiers calculs indiquent que l'approche purement européenne et les différentes options hybrides examinées ci-dessous coûteraient entre 33 et 47 millions d'EUR au démarrage, un montant supplémentaire de 7 à 11 millions d'EUR étant nécessaire pour couvrir les frais de fonctionnement annuels. Les différentes options sont décrites ci-dessous au point 6 de la présente communication. L'option 3 serait la plus onéreuse: 43 millions d'EUR au démarrage pour l'UE et 3,7 millions d'EUR pour l'ensemble des États membres, plus 4,2 millions d'EUR de frais de fonctionnement annuels pour l'UE et 6,8 millions d'EUR pour l'ensemble des États membres. L'option 2 serait la moins coûteuse: 33 millions d'EUR au démarrage pour l'UE et 3,5 millions d'EUR de frais de fonctionnement annuels au niveau de l'UE, plus 3,3 millions d'EUR de frais de fonctionnement annuels pour l'ensemble des États membres. L'option 1 nécessiterait 40,5 millions d'EUR au démarrage pour l'UE et 4 millions d'EUR de frais de fonctionnement annuels au niveau de l'UE, plus 5 millions d'EUR de frais de fonctionnement annuels pour l'ensemble des États membres. Bien entendu, ces coûts diminueront si l'on peut recourir au personnel d'organismes existants, à des infrastructures en place ou à des logiciels et matériels informatiques déjà disponibles. Le coût de la mise en place et de la gestion d'un système purement national serait sensiblement plus élevé (390 millions au démarrage et 37 millions de frais de fonctionnement annuels), car tous les États membres seraient tenus de créer un système de traitement des données hautement sécurisé et d'employer du personnel pour le faire fonctionner.

Ces montants ont un caractère préliminaire et devront faire l'objet d'une analyse approfondie et être précisés au regard des conclusions de l'analyse d'impact.

5. ÉLEMENTS A PRENDRE EN CONSIDERATION

Quelle que soit l'option choisie pour mettre en place et faire fonctionner un SSFT de l'UE, il convient de prendre en considération un certain nombre d'éléments relatifs au champ d'application d'un éventuel SSFT de l'UE. Ils seront examinés ci-après.

5.1. Champ d'application limité au terrorisme et à son financement, ou champ d'application plus vaste?

L'accès aux données de messagerie financière ne trouve pas son utilité uniquement dans le cadre de la lutte contre le terrorisme et son financement. Il ne fait guère de doute qu'accéder à de telles données permettrait aussi de combattre plus efficacement d'autres formes graves de criminalité, en particulier la criminalité organisée et le blanchiment de capitaux. Cependant, dans le contexte de l'accord TFTP UE-USA, les exigences en matière de proportionnalité ont conduit à limiter scrupuleusement l'utilisation des données à la lutte contre le terrorisme et son financement. Il ressort des débats préliminaires qui se sont déroulés jusqu'à présent qu'un large consensus se dégage au sujet du fait que cet argument de la proportionnalité incite également à prévoir un champ d'application tout aussi restreint pour le système équivalent européen, conformément aux exigences générales en matière de respect des droits fondamentaux dont il est question au point 2 de la présente communication.

5.2. Faut-il prévoir plusieurs prestataires, ou limiter le champ d'application à un seul prestataire?

À l'heure actuelle, l'accord TFTP UE-USA prévoit que les demandes de données ne sont adressées qu'à un seul prestataire de services de messagerie financière internationale. Bien que ce prestataire soit de toute évidence le plus important prestataire de services de messagerie de ce type au niveau mondial, d'autres prestataires sont également présents sur le marché. Des considérations relatives à l'efficacité et la nécessité de mettre l'ensemble des acteurs du marché sur un pied d'égalité plaident pour la mise en place d'un système applicable à tous les prestataires de services de messagerie financière internationale. En tout état de cause, il convient de tenir compte de la charge administrative qui pèsera sur les entreprises fournissant des services de messagerie financière au moment de faire un choix entre les différentes options possibles.

5.3. Accord applicable aux seuls services de messagerie internationale, ou également aux services de messagerie nationale?

À l'heure actuelle, l'accord TFTP UE-USA prévoit que les demandes de données ne sont adressées qu'aux prestataires de services de messagerie financière internationale, c'est-à-dire les services de messagerie utilisés pour effectuer des transactions transnationales, y compris entre les États membres mais à l'exclusion de la messagerie financière portant sur des données liées à l'espace unique de paiements en euros (SEPA). Aux fins d'un SSFT de l'UE, il convient de réfléchir également à la possibilité d'inclure ou non les services de messagerie financière échangés entre les États membres, ou de voir s'il est préférable que le SSFT soit limité aux échanges internationaux de services de messagerie financière. Les services de messagerie financière à caractère purement national (utilisés uniquement dans le cadre de transactions financières nationales) sont actuellement exclus du champ d'application de l'accord TFTP UE-USA. Accéder aux données échangées dans le cadre de tels services de messagerie financière nationale serait utile pour lutter contre le terrorisme et d'autres formes de criminalité.

Toutefois, même en faisant abstraction de la question de savoir si l'accès à ces transactions purement nationales doit être réglementé à l'échelon européen, les discussions préliminaires ont confirmé qu'un accès à ces transactions était jugé disproportionné par de nombreux participants aux discussions; il convient donc d'exclure ces transactions du champ d'application d'un système propre à l'UE.

5.4. Sur quel type de données de messagerie financière le système doit-il porter?

Les types de données de messagerie financière utilisées par le système bancaire international sont légion. L'accord TFTP UE-USA se limite actuellement à un type particulier de données de messagerie financière. Accéder à d'autres types de données de messagerie financière serait utile pour lutter contre le terrorisme et son financement et, éventuellement, d'autres formes de criminalité. Cependant, sur ce point également, les considérations liées à la proportionnalité et à la nécessité de respecter les droits fondamentaux des citoyens plaident en faveur d'une limitation des types de messages relevant du champ d'application du système. L'analyse d'impact contiendra des informations plus détaillées concernant cette question technique.

6. OPTIONS ENVISAGEABLES POUR LA MISE EN PLACE D'UN SSFT DE L'UE

Les options décrites ci-dessous sont actuellement examinées par la Commission dans le cadre de l'analyse d'impact qui est en cours. Elles ne sont pas nécessairement limitatives et ne préjugent en aucun cas de la version finale de l'analyse d'impact ni du choix que la Commission posera sur la base de cette analyse.

L'une des options qui est systématiquement envisagée lors de la préparation d'une nouvelle initiative et de l'analyse d'impact qui l'accompagne est l'option du statu quo, ce qui, dans le cas présent, signifierait de maintenir en place l'accord TFTP UE-USA et de ne présenter aucune proposition visant à créer un SSFT de l'UE. Cette option ne permettrait pas de répondre à l'invitation lancée par le Conseil et le Parlement à la Commission de présenter une proposition afin de soumettre «un cadre légal et technique pour l'extraction des données sur le territoire européen», mentionnée au point 1 de la présente communication. En outre, cette option ne contribuerait pas à limiter le volume des données à caractère personnel transférées à des pays tiers et ne permettrait pas davantage de traiter les données sur le territoire de l'UE, dans le respect de la législation et des principes de l'UE en matière de protection des données. Les autres options examinées de manière plus détaillée ci-dessous présentent toutes différentes manières de mettre en place un SSFT de l'UE.

En théorie, l'ensemble des fonctions de base d'un SSFT de l'UE énumérées au point 3 de la présente communication pourraient être mises en œuvre soit au niveau de l'UE, soit au niveau national. Ces fonctions peuvent également être confiées à un ou plusieurs organismes, dans le cadre de leur mandat actuel, ou à de nouveaux organismes qui pourraient être créés afin de remplir ces fonctions. Ces organismes pourraient être soit européens, soit nationaux. Un tel choix implique que – en théorie également – une approche exclusivement européenne est possible, l'ensemble des fonctions de base étant attribuées à des organismes à l'échelon de l'UE, au même titre qu'une approche exclusivement nationale, toutes les fonctions étant confiées à des organismes au niveau national. À titre général, il convient de ne pas perdre de vue que le choix d'un système centralisé, décentralisé ou hybride dans ce dossier précis ne sera pas nécessairement le même que le choix posé dans le cadre d'autres initiatives impliquant le traitement de données aux fins de la lutte contre le terrorisme et la criminalité organisée, chaque initiative dans ce domaine devant être appréciée individuellement.

L'approche purement centralisée et l'approche purement nationale présentent toutes deux des désavantages importants. Ainsi, une approche exclusivement européenne pâtirait certainement du fait qu'elle serait déconnectée des instances et pratiques des États membres dans le domaine de l'action répressive et du renseignement et, partant, manquerait d'efficacité. Sans la contribution des autorités nationales chargées de traiter ces questions, il serait presque impossible de déterminer avec précision les catégories de données devant être demandées au(x) prestataire(s) désigné(s). L'utilité du système serait également amoindrie si l'interrogation de la base de données n'était possible que sur la base d'éléments de renseignement disponibles au niveau de l'UE; au niveau actuel d'intégration de l'UE, ce type d'éléments de renseignement n'est, dans une large mesure, disponible qu'au niveau national. En outre, il est peu probable que les États membres acceptent une approche exclusivement européenne, car elle n'apporterait aucune valeur ajoutée à leurs propres efforts de lutte contre le terrorisme et son financement. Au cours des consultations qui ont été menées, les États membres ont également fait savoir que cette option serait politiquement difficile à accepter pour des motifs d'ordre juridique et opérationnel.

À l'autre extrême, une approche purement nationale ferait courir le risque d'une mise en œuvre divergente dans les différents États membres, et accroîtrait la menace d'atteintes à la sécurité des données, en raison de la nécessité de disposer de 27 copies des données fournies. Une approche purement nationale entraînerait aussi des difficultés relatives à la mise en œuvre d'un cadre harmonisé en matière de protection des données, ainsi que d'une approche harmonisée des autres restrictions nécessaires (et/ou de leur contrôle), comme la limitation du champ d'application du système au terrorisme et à son financement. En outre, une approche exclusivement nationale ne permettrait pas de connaître avec certitude l'État membre chargé de répondre aux demandes de recherches présentées par des pays tiers, et l'avantage supplémentaire que présente l'analyse des résultats des recherches au niveau européen serait perdu. De surcroît, comme indiqué ci-dessus, les coûts associés à cette option seraient nettement plus élevés, puisque l'ensemble des États membres seraient tenus de mettre en place des systèmes de traitement de données hautement sécurisés et d'engager du personnel pour faire fonctionner le système.

Les travaux préparatoires avec les parties prenantes ont par conséquent rapidement montré que les solutions situées aux extrémités de l'éventail des options envisageables ne recueillaient aucun soutien: un consensus s'est dégagé, selon lequel une solution hybride, impliquant de répartir les différentes fonctions entre divers organismes au niveau de l'UE et au niveau national, était la solution la plus susceptible de donner les meilleurs résultats possibles au regard des deux objectifs principaux. Bien que ce consensus permette de déterminer l'option la plus adaptée, l'approche hybride implique encore un grand nombre de choix. Les sections ci-dessous décrivent d'une manière plus détaillée les trois options hybrides qui se sont dégagées des travaux préparatoires actuels comme étant les plus plausibles; ces options sont également présentées dans un tableau en annexe.

6.1. Le service de coordination et d'analyse du SSFT de l'UE (option 1)

Cette option impliquerait de mettre en place une unité centrale européenne du SSFT, la plupart des tâches et fonctions étaient mises en œuvre au niveau de l'UE. Toutes les fonctions – à savoir l'envoi des demandes de données «brutes» au(x) prestataire(s) désigné(s), la vérification de ces demandes, le traitement des demandes de recherches et la réalisation des recherches, la gestion des résultats des recherches et la transmission des rapports aux instances ayant demandé les recherches – se feraient au niveau de l'UE. Toutefois, la préparation des demandes à transmettre au(x) prestataire(s) désigné(s) pourraient se faire en

concertation avec les autorités responsables des États membres, ces derniers pouvant également choisir de détacher leurs propres analystes auprès de l'unité centrale afin qu'ils participent à la réalisation des recherches. Contrairement à l'option prévoyant un système totalement centralisé, les États membres pourraient demander que des recherches soient effectuées en leur nom, comme dans le cadre de la procédure actuellement en place pour le TFTP des États-Unis, ou qu'elles soient effectuées par leurs propres analystes.

Les États membres se trouveraient dans l'obligation de partager des informations avec l'unité centrale européenne du SSFT afin de «motiver» la demande et d'établir le lien entre la demande et le terrorisme avant qu'une recherche ne puisse être commencée, ou de faire valider préalablement leur demande par les autorités nationales. Ces autorités nationales pourraient par exemple être les juges d'instruction ou les procureurs chargés de la lutte contre le terrorisme au niveau national; lorsque ces autorités auraient approuvé une recherche dans les données fournies, l'unité centrale européenne du SSFT pourrait accepter d'effectuer cette recherche sans autre vérification. Selon ce scénario, aucun renseignement supplémentaire ne devrait être communiqué à l'unité centrale européenne du SSFT. Cette dernière transmettrait les résultats des recherches et l'analyse de ceux-ci, et pourrait aussi fournir spontanément des informations. Les États-Unis et les autres pays tiers devraient également introduire une demande pour que des recherches soient effectuées, selon une procédure analogue.

Le suivi du respect des garanties et les contrôles seraient également centralisés, en recourant éventuellement à une surveillance par des acteurs externes, représentant par exemple le(s) prestataire(s) désigné(s) et les instances nommées comme contrôleurs indépendants. La sécurité, l'intégrité et la protection des données seraient également garanties au niveau central.

Les instances clés du système pourraient être Europol et Eurojust. Il conviendrait que les tâches que devraient exécuter Europol et Eurojust s'inscrivent, dans ce cas, dans le droit fil de leurs missions respectives telles que définies par le traité sur le fonctionnement de l'Union européenne (TFUE). En outre, il y aura lieu de déterminer dans quelle mesure il faudra modifier les instruments juridiques régissant actuellement leur fonctionnement. S'il était choisi comme autorité européenne centrale du SSFT, Europol devrait aussi répondre aux demandes d'accès, de rectification et de verrouillage des données présentées par les personnes concernées, conformément au cadre juridique existant applicable à Europol et aux dispositions en vigueur en matière de protection des données. L'unité centrale européenne du SSFT remplirait sa mission dans le respect du cadre juridique existant, et les recours seraient également examinés conformément aux dispositions juridiques existantes. Au niveau national, les autorités répressives auraient un rôle à jouer pour ce qui est de vérifier et d'autoriser les demandes de recherches. La possibilité de créer de nouvelles instances nationales pourrait être envisagée, mais il est préférable de laisser ce choix aux États membres en vertu du principe de subsidiarité[8].

6.2. Le service d'extraction du SSFT de l'UE (option 2)

Comme la première, la deuxième option nécessiterait de mettre en place une unité centrale européenne du SSFT, qui aurait notamment pour mission d'envoyer les demandes de données «brutes» au(x) prestataire(s) désigné(s), la vérification de ces demandes, la réalisation des recherches et le traitement des demandes de recherches. Toutefois, dans le cadre de cette

[8] À ce stade, les conséquences pour les budgets des agences de l'UE susceptibles de jouer un rôle dans la mise en œuvre du système ne sont pas encore connues.

option, l'unité centrale européenne du SSFT ne serait pas autorisée à analyser les résultats des recherches et à les comparer avec d'autres informations ou d'autres éléments de renseignement disponibles lorsque ces recherches sont effectuées à la demande des autorités des États membres; en pareils cas, son rôle se limiterait à préparer et à diffuser les résultats des recherches sous un format adéquat.

Comme dans le cas de l'option 1, les demandes de données «brutes» à adresser au(x) prestataire(s) désigné(s) seraient préparées en étroite concertation avec les États membres, qui pourraient faire connaître leurs besoins spécifiques à l'unité centrale du SSFT, cette dernière étant chargée de les analyser et de formuler la ou les demandes en fonction de son analyse.

Les autorités des États membres demanderaient que des recherches soient effectuées en leur nom. Le bien-fondé de ces recherches et leur lien avec le terrorisme seraient vérifiés et validés au niveau national. L'unité centrale européenne du SSFT effectuerait les recherches et renverrait l'ensemble des résultats, présentés sous un format adéquat, aux États membres. Les autorités des États membres seraient les seules à procéder à l'analyse des recherches, et elles pourraient également choisir de fournir des informations à titre spontané.

L'unité centrale européenne du SSFT serait chargée de procéder aux recherches et d'en analyser les résultats au nom des institutions de l'UE, des États-Unis et d'autres pays tiers. Elle pourrait aussi fournir des informations spontanément sur cette base.

Comme dans le cadre de l'option précédente, le suivi du respect des garanties et les contrôles seraient centralisés, en recourant éventuellement à une surveillance assurée par des acteurs externes, représentant par exemple le(s) prestataire(s) désigné(s) et les instances nommées comme contrôleurs indépendants. La sécurité, l'intégrité et la protection des données seraient également garanties au niveau central.

Comme dans l'option précédente également, les instances clés du système pourraient être Europol et Eurojust. Au niveau national, les instances clés seraient les autorités nationales répressives ou chargées du renseignement. Comme pour l'option précédemment examinée, la décision de créer de nouvelles instances nationales serait laissée aux États membres en vertu du principe de subsidiarité. Europol et/ou les unités nationales répondraient aux demandes d'accès, de rectification et de suppression des données présentées par les citoyens de l'Union, avec le concours tant des autorités nationales chargées de la protection des données que de l'autorité de contrôle commune d'Europol. Les recours seraient examinés conformément aux dispositions juridiques applicables au niveau national ou au niveau de l'UE[9].

6.3. Le service de coordination des cellules de renseignement financier (CRF) (option 3)

Cette option impliquerait la mise en place d'un forum modernisé des CRF, composé de l'ensemble des CRF des États membres. L'autorité ad hoc au niveau de l'UE adresserait des demandes de données «brutes» au(x) fournisseur(s) désigné(s), en rassemblant, dans une demande unique, les besoins exprimés par les CRF, qui serait également vérifiée et autorisée au niveau central.

Chaque CRF serait chargée d'effectuer les recherches et de gérer les résultats des recherches au nom de son État membre, ainsi que de procéder aux analyses et de transmettre les rapports

[9] Voir la note de bas de page n° 8.

aux instances qu'elle estimerait concernées. Le bien-fondé de ces recherches et leur lien avec le terrorisme seraient vérifiés et validés au niveau national ou de l'UE. Les CRF seraient également chargées de fournir spontanément des informations.

Le forum modernisé des CRF serait en mesure d'effectuer des recherches et d'analyser les résultats au nom des institutions de l'UE et d'autres pays tiers avec lesquels l'UE aurait conclu un accord. Il pourrait aussi fournir aussi des informations spontanément.

Le suivi du respect des garanties et les contrôles seraient centralisés, en recourant éventuellement à une surveillance assurée par des acteurs externes, représentant par exemple le(s) prestataire(s) désigné(s) et les instances nommées comme contrôleurs indépendants. La sécurité, l'intégrité et la protection des données seraient également garanties au niveau central.

Le forum modernisé des CRF se verrait accorder un statut juridique officiel, son rôle et ses responsabilités étant clairement définis. Au niveau national, les instances clés seraient les CRF et les autorités nationales répressives et chargées du renseignement.

Une autorité au niveau de l'UE traiterait les demandes d'accès, de rectification et de suppression des données présentées par les citoyens de l'UE, les recours étant examinés conformément aux dispositions juridiques applicables au niveau national ou de l'UE.

7. CONCLUSIONS

Sur la base des travaux préparatoires menés par la Commission à ce jour, et sous réserve des résultats de l'analyse d'impact, la présente communication décrit les différentes options envisageables pour la création d'un «cadre légal et technique pour l'extraction des données sur le territoire européen» dans le contexte d'un système de surveillance du financement du terrorisme. Les différentes options proposées dans la présente communication montrent que des choix et des décisions d'importance seront encore nécessaires, notamment en ce qui concerne le respect des droits fondamentaux, et que de nombreux aspects juridiques, techniques, organisationnels et financiers devront être examinés d'une manière beaucoup plus détaillée au cours des travaux préparatoires complémentaires. Compte tenu de la difficulté de la tâche, la Commission estime qu'il convient de prévoir un délai suffisant pour les travaux préparatoires complémentaires et le débat avec le Conseil et le Parlement.

* * *

Annexe: présentation sous forme de tableau des options hybrides

	Service de coordination et d'analyse du SSFT de l'UE (option 1)	Service d'extraction du SSFT de l'UE (option 2)	Service de coordination des cellules de renseignement financier (CRF) (option 3)
Préparation et envoi des demandes de «données brutes»	Unité centrale européenne du SSFT en concertation avec les États membres	Unité centrale européenne du SSFT en concertation avec les États membres	Forum modernisé des CRF
Contrôle et autorisation des demandes de «données brutes»	Eurojust ou un autre organe existant	Eurojust ou un autre organe existant	Eurojust ou un autre organe existant
Réception et stockage des «données brutes», sécurité des données	Europol ou un autre organe de l'UE comme l'agence chargée des systèmes d'information	Europol ou un autre organe de l'UE comme l'agence chargée des systèmes d'information	Europol ou un autre organe de l'UE comme l'agence chargée des systèmes d'information
Réalisation des recherches sur les «données brutes»	Unité centrale européenne du SSFT, analystes détachés par les États membres ou combinaison de ces deux ressources	Unité centrale européenne du SSFT	CRF, Forum modernisé des CRF
Contrôle et autorisation de la réalisation des recherches	Contrôleurs indépendants, éventuellement autorités nationales	Contrôleurs indépendants, autorités nationales	Contrôleurs indépendants
Analyse des résultats des recherches	Unité centrale européenne du SSFT, analystes détachés par les EM ou combinaison de ces deux ressources	Autorités nationales pour les recherches nationales, analystes de l'unité centrale européenne du SSFT pour les recherches au niveau de l'UE et concernant les pays tiers	Forum modernisé des CRF, CRF nationales
Diffusion des résultats des	Analystes d'Europol ou analystes détachés	Autorités nationales pour les recherches	Forum modernisé des CRF, CRF nationales

recherches	par les États membres	nationales, analystes de l'unité centrale européenne du SSFT pour les recherches au niveau de l'UE et concernant les pays tiers	
Définition d'un régime adéquat de protection des données	Europol ou un autre organe de l'UE comme l'agence chargée des systèmes d'information	Europol ou un autre organe de l'UE comme l'agence chargée des systèmes d'information	Europol ou un autre organe de l'UE comme l'agence chargée des systèmes d'information