CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 29 juin 2007 (12.07)
(OR. en)

10741/2/07
REV 2

JAI 319
ECOFIN 270

DÉCLASSIFICATION

du document:	ST 10741/1/07 REV1 RESTREINT UE
en date du:	22 juin 2007
nouvelle classification:	sans classification
Objet:	Traitement par le département du Trésor des États-Unis, aux fins de la lutte contre le terrorisme, de données à caractère personnel provenant de l'UE - "SWIFT"

Les délégations trouveront ci-joint la version déclassifiée du document cité en objet.

Le texte de ce document est identique à celui de la version précédente.

CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 22 juin 2007 (11.07)
(OR. en)

10741/1/07
REV 1

RESTREINT UE

JAI 319
ECOFIN 270

NOTE

de:	la Commission
aux:	délégations
Objet:	Traitement par le département du Trésor des États-Unis, aux fins de la lutte contre le terrorisme, de données à caractère personnel provenant de l'UE - "SWIFT"

1. CONTEXTE ET HISTORIQUE DU DOSSIER

Après les attentats du 11 septembre 2001, le département du Trésor des États-Unis "département du Trésor" a mis au point un programme de surveillance du financement du terrorisme ("Terrorist Finance Tracking Program" - ci-après dénommé "TFTP"). Ce programme se fonde sur des mandats légaux et des décrets présidentiels autorisant le département du Trésor à recourir à des mesures appropriées pour identifier, localiser et poursuivre les soutiens financiers du terrorisme.

Des articles de presse parus en juin 2006 ont révélé que le Bureau de contrôle des avoirs étrangers (Office of Foreign Assets Control - OFAC) du département du Trésor, agissant en vertu des compétences qui lui sont conférées au titre du TFTP, avait adressé des injonctions administratives à SWIFT (Society for Worldwide Interbank Financial Telecommunication)[1] pour exiger des bureaux de cette société implantés aux États-Unis qu'ils transfèrent à l'OFAC des données à caractère personnel conservées sur leur serveur[2] installé aux États-Unis, ces données devant servir à agir contre des personnes ou des entités faisant l'objet de soupçons dans le cadre de la lutte contre le terrorisme.

D'après le département du Trésor, l'utilisation des données traitées par SWIFT a renforcé la capacité des États-Unis et de pays tiers à identifier les financiers du terrorisme, à dresser un état des réseaux terroristes et à désorganiser les activités des terroristes et de leurs sympathisants.

Immédiatement après la divulgation de ces faits par la presse, l'autorité belge chargée de la protection des données a rendu le 27 juillet 2006 un avis précisant que les activités de traitement menées par SWIFT pour l'exécution des paiements interbancaires violaient la loi belge en matière de protection des données, qui transpose la directive 95/46/CE relative à la protection des données à caractère personnel ("directive relative à la protection des données")[3]. Dans l'avis qu'elle a rendu, l'autorité belge chargée de la protection des données a répertorié diverses atteintes aux principes fondamentaux régissant la protection des données, en rapport notamment avec le transfert de données à caractère personnel vers des pays tiers. Les discussions en cours entre SWIFT et cette autorité visent à ce que la société se conforme à la législation belge en matière de protection des données.

---

1 SWIFT est une société basée en Belgique qui dispose de bureaux aux États-Unis et exploite un système mondial de messagerie utilisé pour transmettre notamment des informations sur les transactions bancaires. D'après les estimations, SWIFT traite 80 % du trafic mondial des transferts électroniques de valeurs.

2 Pour des raisons de sécurité des données, SWIFT exploite deux serveurs "miroirs" identiques, l'un situé dans l'Union européenne et l'autre aux États-Unis. Toutes les données de messagerie financière sont conservées sur chaque serveur pendant 124 jours.

3 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31 à 50).

À la fin du mois de novembre 2006, le Groupe de l'article 29 (l'organe consultatif indépendant auprès de la Commission européenne pour les questions de protection des données et de vie privée) a rendu un avis sur le traitement, par SWIFT, des données à caractère personnel. La conclusion de cet avis est que SWIFT et les institutions financières qui utilisent ses services ont violé la législation communautaire en matière de protection des données telle qu'énoncée dans la directive 95/46/CE, notamment en n'ayant pas assuré une protection adéquate dans le cadre du transfert de données à caractère personnel vers les États-Unis et en n'ayant pas informé les personnes concernées de la manière dont les données à caractère personnel les concernant ont été traitées. Le Groupe de l'article 29 continue de suivre ces questions et coordonne les actions engagées au niveau national par les autorités de contrôle de la protection des données.

Le cadre juridique actuel de l'UE en matière de protection des données prévoit un instrument particulier pour les transferts de données à caractère personnel vers les États-Unis: en application de l'article 25, paragraphe 6, de la directive 95/46/CE relative à la protection des données, la Commission a adopté le 26 juillet 2000 une décision relative à la pertinence de la protection assurée par les principes de la "sphère de sécurité" [4]. La Commission y indique que ces principes assurent un niveau de protection adéquat pour le transfert de données de la Communauté vers les États-Unis. Cette reconnaissance du niveau adéquat de protection ne s'applique qu'aux entreprises certifiant qu'elles respecteront les principes précités.

2. ÉTAT ACTUEL DU DOSSIER

SWIFT et les autorités concernées des États-Unis sont entrées dans la phase finale de leurs discussions relatives à l'adhésion à la "sphère de sécurité", qui permettrait à SWIFT de transférer vers les États-Unis des données à des fins commerciales. SWIFT devrait être en mesure d'adhérer à la "sphère de sécurité" d'ici début juillet 2007. Par ailleurs, SWIFT et ses clients (banques) déterminent actuellement les mesures qu'il convient de prendre pour que les clients, qu'il s'agisse de banques ou d'institutions financières, soient informés de manière appropriée sur le traitement des données détenues par SWIFT, y compris les transferts vers les États-Unis à des fins commerciales et le traitement éventuel de ces données par le département du Trésor aux fins de la lutte contre le terrorisme.

---

[4] Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (2000/520/CE).

Les principes de la "sphère de sécurité", qui sont destinés à protéger les données à caractère personnel, prévoient que l'adhésion auxdits principes peut être limitée par "les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis"[5]. Les États-Unis doivent donc être en mesure de prouver que toute limitation aux principes de la "sphère de sécurité" qu'ils imposeraient pour des raisons de sécurité nationale ou de respect de leurs lois est nécessaire et proportionnée. À cet effet, la Commission, avec le concours de la présidence du Conseil[6], a discuté, avec le département du Trésor, d'un ensemble d'"observations" (voir annexe), dans le cadre desquelles le département du Trésor s'engage unilatéralement à traiter les données à caractère personnel provenant de l'UE dans le respect des principes en vigueur dans l'Union pour la protection des données. Le Parlement (Commission des libertés civiles, de la justice et des affaires intérieures) et le Conseil (COREPER) ont été régulièrement tenus au courant de ces discussions[7], de même que le Groupe de l'article 29[8].

Les observations prévoient des garanties pour le traitement des données à caractère personnel provenant de l'UE que la société SWIFT est tenue de communiquer en vertu d'une injonction du département du Trésor[9]. À ce titre, par exemple, le département du Trésor s'engage à utiliser les données communiquées par SWIFT exclusivement dans le cadre d'enquêtes relevant de la lutte contre le terrorisme et à ne pas consulter les données à d'autres fins. Les observations prévoient des assurances importantes concernant la sécurité des données de SWIFT que le Trésor détient, les restrictions d'accès aux données de SWIFT, les conditions dans lesquelles les informations produites par SWIFT peuvent être mises en commun avec d'autres services officiels américains et l'utilisation que ces services peuvent faire de ces données. Dans les observations, le Trésor des États-Unis s'engage aussi à analyser en permanence les données qu'il détient afin de répertorier et d'effacer les données qui ne sont pas nécessaires aux fins du programme TFTP et à ne pas conserver les données pendant une durée supérieure aux délais fixés[10]. Pour permettre un suivi effectif des observations, la Commission, en accord avec le département du Trésor, désignera une personnalité européenne éminente, qui sera chargée, en qualité de tiers indépendant, de contrôler le respect des engagements figurant dans les observations; elle fera rapport à la Commission, qui, à son tour, rendra compte au Parlement européen et au Conseil.

---

5 ANNEXE I de la décision de la Commission du 26 juillet sur les principes de la "sphère de sécurité".

6 Dans son arrêt rendu le 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 ("arrêt PNR"), la Cour de justice a considéré que l'accès direct des services répressifs aux données à caractère personnel ne peut pas être réglementé au niveau communautaire. La situation dans le cas de SWIFT est différente de celle à laquelle l'arrêt PNR s'applique puisque, s'agissant de SWIFT, les données à caractère personnel sont transférées vers les États-Unis à des fins commerciales (les autorités de ce pays n'ont éventuellement accès à ces données qu'ultérieurement, sur leur territoire) tandis que, dans le cas des données PNR, la Cour a considéré que le transfert direct vers les autorités américaines intervenait exclusivement à des fins répressives.

7 En 2007, le dossier "SWIFT" a été inscrit à l'ordre du jour des sessions restreintes du COREPER des 21 février, 14 mars, 11 mai et 30 mai.

8 Lors de ses réunions plénières des 14 et 15 février ainsi que des 18 et 19 avril 2007.

9 L'examen de ces garanties a été engagé sur la base d'un courrier confidentiel entre le département du Trésor et SWIFT, dans lequel le premier accepte un certain nombre de limitations et de contrôles concernant le traitement des données de SWIFT.

10 Il est envisagé de publier les observations à la fois au Registre fédéral américain ("US Federal Register") et au Journal officiel. Les données reçues par le département du Trésor après la date de publication seront conservées pendant cinq ans maximum à compter de la date de réception. Les données reçues par le département du Trésor avant la date de publication seront conservées pendant cinq ans maximum à compter de la date de publication.

Le respect des garanties énoncées dans les observations du département du Trésor devrait contribuer à témoigner du caractère proportionné du traitement, par le département précité, des données à caractère personnel provenant de l'UE et stockées sur le serveur de SWIFT implanté aux États-Unis, que cette société est tenue de communiquer en vertu d'une injonction.

***

ANNEXE

21 juin 2007 - Texte final

Programme de surveillance du financement du terrorisme

Observations du Département du Trésor des États-Unis

Les présentes observations décrivent le programme de surveillance du financement du terrorisme (Terrorist Financing Tracking Program - TFTP) du département du Trésor des États-Unis ("département du Trésor") et, en particulier, les contrôles rigoureux et les garanties qui régissent le traitement, l'utilisation et la communication des données transmises par SWIFT en vertu d'une injonction administrative. Ces contrôles et garanties s'appliquent à toutes les personnes qui ont accès aux données SWIFT, sauf indication contraire dans des exemples précis tels que ceux décrivant l'échange d'informations essentielles extraites des données SWIFT avec des gouvernements étrangers.

Le TFTP est doté d'un fondement légal, il est soigneusement ciblé, puissant et efficace, et il est lié par le principe de protection de la vie privée. Il correspond exactement à ce que les citoyens espèrent que leur gouvernement fera pour les protéger contre les menaces terroristes.

Le programme de surveillance du financement du terrorisme du département du Trésor

Peu après les attentats du 11 septembre 2001, dans le cadre des efforts mis en œuvre pour employer tous les moyens disponibles en vue de repérer les terroristes et leurs réseaux, le département du Trésor a lancé le TFTP, au titre duquel il a adressé des injonctions administratives au centre d'exploitation de la Société de télécommunications interbancaires mondiales ("Society for Worldwide Interbank Financial Telecommunication" (SWIFT) aux États-Unis en vue d'obtenir des données liées au terrorisme; SWIFT est une société coopérative de droit belge qui fournit un service mondial de messagerie financière utilisé pour la transmission d'informations sur les opérations financières. En vertu de ces injonctions, SWIFT doit communiquer au département du Trésor certains historiques d'opérations financières - qui sont tenus par le centre d'exploitation de SWIFT aux États-Unis dans le cadre de l'exercice normal de son activité - destinés à être utilisés exclusivement à des fins de lutte contre le terrorisme, comme indiqué dans les points suivants.

Principes fondamentaux sous-tendant le TFTP

Dès le départ, le TFTP a été conçu et mis en œuvre pour satisfaire aux exigences légales des États-Unis, contribuer de manière efficace à la lutte contre le terrorisme mondial et respecter et protéger le caractère potentiellement sensible sur le plan commercial des données SWIFT détenues aux États-Unis ainsi que leur confidentialité. Le TFTP tient compte du caractère potentiellement sensible sur le plan commercial ainsi que de la protection de la confidentialité des informations qu'il traite, et les garanties énoncées dans les présentes observations s'appliquent, quelle que soit la nationalité ou le lieu de résidence des personnes concernées. Le programme comporte de multiples niveaux de contrôles gouvernementaux et indépendants qui se couvrent partiellement, afin de garantir que les données, qui sont restreintes par nature, ne soient utilisées qu'aux fins exclusives de la lutte contre le terrorisme et qu'elles soient toutes conservées dans un environnement sécurisé et fassent l'objet d'un traitement adéquat.

Toutes les actions menées par le département du Trésor en vue d'obtenir des informations particulières de la part du centre d'exploitation de SWIFT situé aux États-Unis et de les utiliser exclusivement aux fins d'enquête, de détection, de prévention et/ou de poursuites dans le cadre de la lutte contre le terrorisme ou son financement, ou d'enquêtes et de poursuites qui en résultent, sont conformes avec le droit américain. Par ailleurs, les données communiquées par SWIFT ne sont pas utilisées pour recueillir des preuves ou détecter une activité sans lien avec le terrorisme ou son financement, même si cette activité en tant que telle peut être illégale. Le département du Trésor n'utilise pas les données SWIFT dans le cadre d'enquêtes générales dans le domaine de la fraude fiscale, du blanchiment de capitaux, de l'espionnage économique, du trafic de stupéfiants ou d'une autre activité criminelle, et ces données ne peuvent d'ailleurs pas être utilisées dans ce cadre, sauf si, dans des cas particuliers, l'une de ces activités se trouve avoir un lien avec le terrorisme ou son financement.

Les données communiquées par SWIFT en vertu d'une injonction sont des copies de messages d'opérations financières effectuées, c'est-à-dire des copies d'historiques d'activités conservés au centre d'exploitation de SWIFT aux États-Unis dans le cadre de l'exercice normal de son activité. Bien que ces données puissent faire l'objet d'un traitement aux fins de la recherche très limitée axée sur la lutte antiterroriste qui est décrite ici, il n'est effectué aucune modification, manipulation, adjonction ou suppression de données sur les messages de transactions qui se trouvent dans la base de données interrogeable.

Le TFTP a prouvé son efficacité en tant qu'outil d'investigation et il a largement contribué à protéger des citoyens des États-Unis et d'autres personnes dans le monde entier et à préserver la sécurité nationale des États-Unis et d'autres pays. Ce programme a contribué à identifier et à arrêter des terroristes et leurs financiers, et il a permis d'obtenir de nombreux indices qui ont été communiqués aux experts de la lutte contre le terrorisme des services de renseignement et de police du monde entier.

Préoccupations exprimées au sein de l'Union européenne

À la suite de la révélation de l'existence du TFTP par les médias en juin 2006, des préoccupations ont été exprimées au sein de l'UE au sujet de ce programme et, notamment, quant à la possibilité pour le département du Trésor d'avoir accès à des données à caractère personnel concernant une personne physique identifiée ou identifiable, apparaissant dans les opérations financières traitées par SWIFT. En particulier, des questions ont été posées quant à la compatibilité du TFTP avec les obligations découlant de la directive relative à la protection des données (directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), ainsi que des lois des États membres mettant en œuvre cette directive.

Nature des données SWIFT

Les historiques d'opérations financières communiqués par SWIFT en vertu d'une injonction peuvent comprendre des informations d'identification sur l'émetteur et/ou le bénéficiaire de l'opération, comme le nom, le numéro de compte, l'adresse, le numéro national d'identification, et d'autres données à caractère personnel. Il est tout à fait improbable que les historiques financiers de SWIFT comprennent les données "sensibles" visées à l'article 8 de la directive 95/46/CE (à savoir les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle de la personne concernée).

Principes de la lutte contre le financement du terrorisme international

Les données financières de SWIFT utilisées dans le cadre du TFTP sont extrêmement précieuses pour la lutte contre le terrorisme mondial et son financement, et pour permettre au gouvernement d'assurer sa mission, qui est de défendre la population, de préserver la sécurité nationale, de détecter et de prévenir les actes terroristes et de se charger des enquêtes et des poursuites en la matière.

La communauté internationale et les autorités nationales ont conscience que l'argent est le "nerf" du terrorisme, comme en témoigne la Convention internationale de 1999 des Nations unies pour la répression du financement du terrorisme ainsi que de nombreuses résolutions des Nations unies concernant la prévention et la répression du financement des actes terroristes, notamment la résolution 1373 du Conseil de sécurité des Nations unies. Aux États-Unis, le département du Trésor et le Congrès ont créé en 2004 le Bureau de la lutte anti-terrorisme et du renseignement financier (Office of Terrorism and Financial Intelligence) (ci-après dénommé "Bureau") pour coordonner les services de police et de renseignement au sein du Département dans le double but de protéger le système financier contre un usage illicite et de lutter entre autres contre les terroristes et les autres menaces pour la sécurité nationale. Les différents services du Bureau rassemblent et analysent les informations émanant des services de police et de renseignement ainsi que des institutions financières et portant sur les méthodes employées par les terroristes (et les autres criminels) pour se procurer des capitaux, les transférer et les conserver. Ces activités permettent au Bureau de geler les avoirs des terroristes, de lutter contre le terrorisme en général, et d'élaborer et de promouvoir des normes en matière de lutte contre le financement du terrorisme aux États-Unis et à l'étranger.

Ces initiatives et d'autres encore tiennent compte de la réalité quotidienne des terroristes qui ont besoin d'un flux de trésorerie régulier pour payer les opérationnels, organiser les déplacements, former les nouveaux membres, falsifier des documents, verser des pots de vin, se procurer des armes et planifier des attentats. Lorsqu'ils envoient de l'argent par l'intermédiaire du système bancaire, ils fournissent souvent des informations qui permettent d'obtenir le type d'indices concrets susceptibles de faire progresser une enquête liée au terrorisme. C'est la raison pour laquelle les responsables de la lutte anti-terrorisme accordent un grand intérêt au renseignement financier, notamment aux informations obtenues par le biais de programmes tels que le TFTP, qui s'est avéré d'une valeur inestimable dans la lutte contre le terrorisme mondial.

C'est également pour cette raison que le secteur financier est soumis à des exigences importantes en matière de conservation et de communication des données en vue de soutenir les efforts des gouvernements en matière de lutte contre le terrorisme. Dans le monde entier, les pays ont rendu cette procédure obligatoire, conformément aux recommandations du groupe d'action financière (GAFI). Par exemple, aux États-Unis, l'instrument légal de référence est la loi relative au secret bancaire (Bank Secrecy Act). En Europe, des dispositions similaires ont été mises en œuvre dans le droit national en vertu de la troisième directive sur le blanchiment des capitaux et, plus récemment, du règlement (CE) n°1781/2006 du Parlement européen et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds.

Bases légales permettant d'obtenir et d'utiliser les données SWIFT

Les injonctions adressées à SWIFT se fondent sur des textes de lois établis de longue date et sur un décret présidentiel (executive order) relatif à la lutte contre le terrorisme et son financement. La loi de 1977 sur les pouvoirs économiques en cas d'urgence internationale (International Emergency Economic Powers Act déclaré - IEEPA) autorise le Président des États-Unis, en cas d'état d'urgence nationale déclaré, à ordonner une enquête sur les virements bancaires et autres transactions dans lesquelles un étranger a des intérêts. De même, l'UNPA (United Nations Participation Act de 1945) autorise le Président, dans le cadre de la mise en œuvre des résolutions du Conseil de sécurité des Nations unies, à ordonner une enquête sur les relations économiques ou les moyens de communication entre tout étranger et les États-Unis.

Le 23 septembre 2001, le Président, s'appuyant en partie sur l'IEEPA et l'UNPA et citant les résolutions du Conseil de sécurité des Nations unies concernant les Taliban et Al Qaïda, a signé le décret présidentiel n° 13224. Dans ce décret, le Président déclare le pays en état d'urgence afin de faire face aux attentats terroristes du 11 septembre et à la menace persistante et directe de nouveaux attentats et il bloque les avoirs des personnes qui commettent ou menacent de commettre des actes terroristes, ou qui soutiennent le terrorisme, et interdit les transactions avec celles-ci.

Aux fins du décret présidentiel n° 13224, la section 3 contient la définition suivante:

on entend par "terrorisme" des activités —

i) impliquant des actes violents ou dangereux pour la vie humaine, les biens,ou les infrastructures; et

ii) apparaissant comme destinées —

(A) à intimider ou contraindre une population civile;

(B) à influencer la politique d'un gouvernement par l'intimidation ou la coercition; ou

(C) à nuire à l'action d'un gouvernement par la destruction de masse, l'assassinat, l'enlèvement ou la prise d'otages.

Dans la section 7 du décret présidentiel, le Secrétaire au Trésor est autorisé à employer tous les pouvoirs conférés au Président par l'IEEPA et l'UNPA nécessaires pour l'application du décret. Le Président autorise également le Secrétaire au Trésor à déléguer à son tour une ou plusieurs de ces fonctions à d'autres fonctionnaires ou organismes du gouvernement des États-Unis, et déclare que tous les organismes du gouvernement des États-Unis sont tenus de prendre les mesures appropriées relevant de leur compétence pour mettre en œuvre les dispositions du décret. L'IEEPA et le décret, mis en œuvre par les Global Terrorism Sanctions Regulations, autorisent le directeur du Bureau du contrôle des avoirs étrangers (Office of Foreign Assets Control - OFAC) du département du Trésor à exiger de toute personne qu'elle fournisse des données relatives aux transactions financières ou d'autres données en rapport avec une enquête liée à des sanctions économiques. Tels sont les fondements légaux au titre desquels l'OFAC adresse à SWIFT des injonctions de produire des données financières liées à une enquête sur le terrorisme.

Contrôle des accès et sécurité du système informatique

Conformément aux procédures édictées par le gouvernement des États-Unis pour le traitement des informations liées aux enquêtes sur le terrorisme et, plus généralement, à son financement, les données communiquées par SWIFT sont soumises à des mesures strictes sur le plan technique et de l'organisation afin d'être protégées contre une destruction, une perte, une modification ou un accès accidentels ou illégaux. Toutes les mesures de sécurité qui sont évoquées ci-dessous font l'objet d'un audit indépendant.

Les données de SWIFT sont conservées dans un environnement sécurisé et stockées séparément de toutes les autres données; et les systèmes informatiques sont dotés de systèmes de protection perfectionnés contre l'intrusion, ainsi que d'autres protections afin que l'accès ne puisse avoir lieu que de la manière qui se trouve décrite ici. Il n'est procédé à aucune copie des données de SWIFT, si ce n'est à des fins de sauvegarde et de récupération en cas de catastrophe. L'accès aux données et aux équipements informatiques est limité aux personnes qui disposent des habilitations de sécurité nécessaires. Même pour ces personnes, l'accès aux données de SWIFT ne se fait qu'en lecture seule et est strictement limité par le TFTP, en fonction du besoin d'en connaître, aux analystes spécialisés dans les enquêtes antiterroristes et aux personnes chargées du support technique, de la gestion et de la surveillance du TFTP.

Extraction et utilisation limitées aux enquêtes antiterroristes

Le TFTP ne prévoit pas l'exploration de données ni tout autre type de profilage algorithmique ou informatisé, ou de filtrage. Plusieurs niveaux de contrôles stricts ont été intégrés dans le TFTP pour limiter le nombre d'informations recueillies, garantir que les informations ne soient extraites et utilisées qu'aux fins de la lutte antiterroriste et protéger la vie privée des personnes qui ne sont pas liées au terrorisme ou à son financement. Ces garanties, qui se recouvrent partiellement, circonscrivent continuellement et restreignent considérablement l'accès aux données financières traitées par SWIFT dans ses opérations quotidiennes, ainsi que leur utilisation.

Il convient d'emblée de préciser que les injonctions adressées à SWIFT sont soigneusement et strictement adaptées pour limiter le volume des données transmises au département du Trésor. SWIFT est tenue de communiquer uniquement les données dont le département du Trésor estime qu'elles seront nécessaires pour lutter contre le financement du terrorisme, sur la base d'analyses antérieures centrées sur les types de messages et leur périmètre de sélection, ainsi qu'en fonction de ses observations en matière de menace et de vulnérabilité. Par ailleurs, les recherches sont strictement adaptées pour limiter au maximum l'extraction de messages sans intérêt pour les enquêtes antiterroristes. Les données de SWIFT ne sont utilisées que pour extraire des informations concernant une enquête liée au terrorisme précise et en cours. Il en résulte que, pour effectuer n'importe quelle recherche, il faut indiquer, éléments de preuve fondés à l'appui, que la personne ciblée par cette recherche a un lien avec le terrorisme ou son financement. Toute recherche effectuée sur les données de SWIFT dans le cadre du TFTP est en outre consignée simultanément, y compris l'élément qui a établi un lien incontestable avec le terrorisme et a déclenché la recherche.

Compte tenu de toutes ces garanties, seule une part infime (moins d'un pour cent) des messages communiqués par SWIFT au département du Trésor ont effectivement été consultés et uniquement parce qu'ils répondaient aux critères d'une recherche ciblée en matière de lutte antiterroriste.

Contrôle indépendant

En plus des contrôles décrits ci-dessus, exercés constamment par le Trésor américain, le TFTP comporte plusieurs autres niveaux de contrôle indépendant: par des représentants de SWIFT, par un cabinet d'audit indépendant et par d'autres administrations officielles indépendantes aux États-Unis, parmi lesquelles le Congrès.

SWIFT et les vérificateurs externes qu'elle a choisis exercent un contrôle indépendant du TFTP de plusieurs manières complémentaires. Tout d'abord, des représentants de SWIFT ont reçu une habilitation de sécurité qui leur permet d'avoir accès 24 heures sur 24 aux équipements et aux données et ils peuvent suivre, en temps réel et a posteriori, l'utilisation des données pour s'assurer qu'elles n'ont été consultées qu'à des fins de lutte contre le terrorisme. En outre, ces représentants de SWIFT peuvent mettre fin instantanément à une recherche et sont même en mesure, en cas de doute, d'arrêter tout le système.

La maintenance et l'utilisation des données de SWIFT ainsi que l'accès à celles-ci font l'objet d'un audit périodique indépendant, en application de protocoles soigneusement définis et conformes aux normes d'audit internationales. Ces audits portent sur le contrôle de l'accès et les garanties de sécurité du système informatique, ainsi que sur la limitation de la consultation des données à des fins de lutte contre le terrorisme, comme expliqué ci-dessus. Les vérificateurs indépendants communiquent leurs conclusions au comité chargé de l'audit et des finances du Conseil d'administration de SWIFT (Audit and Finance Committee).

De plus, conformément à la législation des États-Unis, plusieurs commissions du Congrès ont été et sont toujours régulièrement informées sur le TFTP et son fonctionnement. Le TFTP a également fait l'objet d'auditions publiques au Congrès.

Enfin, le Conseil de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board), qui a été institué en application de la loi sur la réforme des services de renseignement et la prévention du terrorisme (Intelligence Reform and Terrorism Prevention Act) de 2004 exerce un contrôle sur le TFTP. Il a pour mission de veiller à ce que les exigences en matière de respect de la vie privée et des libertés civiles soient correctement prises en compte dans la mise en œuvre de l'ensemble des lois, règlements et mesures gouvernementales visant à protéger les États-Unis contre le terrorisme. Ce conseil est également chargé d'analyser les pratiques des différents ministères et agences en matière d'échange d'informations sur le terrorisme pour évaluer si les consignes de protection de la vie privée et des libertés civiles sont bien respectées.

Comme on le lira ci-après, ce contrôle étendu et indépendant va de pair avec des règles strictes en matière de diffusion, qui ont pour effet de restreindre encore l'accès aux informations tirées des historiques financiers de SWIFT et de renforcer la protection de la vie privée.

Communication et échange d'informations

La communauté internationale sait qu'il est essentiel d'échanger les informations concernant le terrorisme. Ainsi, la résolution 1373 du Conseil de sécurité des Nations unies demande à tous les États d'intensifier et d'accélérer l'échange d'informations opérationnelles et d'échanger des renseignements afin de prévenir les actes de terrorisme. De même, en vertu de la section 6 du décret présidentiel n°13224, le Secrétaire au Trésor (et d'autres responsables) doivent tout mettre en œuvre pour coopérer et coordonner leur action avec d'autres pays pour atteindre les objectifs fixés par ce décret, et notamment prévenir et éliminer les actes de terrorisme, empêcher les terroristes d'avoir accès aux services financiers et à des financements, et échanger des renseignements sur les activités de financement du terrorisme. Compte tenu de ce qui précède, les informations tirées des données de SWIFT sont échangées comme il convient avec des partenaires aux États-Unis ou à l'étranger. Comme pour tous les autres aspects du TFTP, ces échanges d'informations se font dans le respect de la législation des États-Unis et moyennant une série de garanties conçues pour protéger les données de SWIFT et la vie privée des personnes qu'elles peuvent concerner.

Les analystes spécialisés dans la lutte antiterroriste qui effectuent des recherches dans le cadre du TFTP vérifient la pertinence des résultats d'une recherche avant que ces informations soient préparées pour être communiquées par des canaux sécurisés. Le département du Trésor exerce aussi un contrôle de l'origine sur la communication ultérieure de ces informations en ce sens que leur destinataire n'est pas autorisé à communiquer les informations à d'autres personnes sans l'accord exprès du département du Trésor. Comme pour tout autre accès non autorisé aux données de SWIFT, toute divulgation non autorisée d'informations tirées du TFTP peut donner lieu à de sévères mesures disciplinaires ou à des sanctions civiles ou pénales.

Les informations tirées des données de SWIFT font l'objet d'échanges strictement contrôlés avec d'autres services américains dans le secteur de la police et du renseignement; ces informations ne doivent être utilisées qu'aux fins d'enquête, de détection, de prévention et/ou de poursuites dans le cadre de la lutte contre le terrorisme ou son financement, ou d'enquêtes et de poursuites qui en résultent. Ces échanges d'informations sont requis par la loi sur la sécurité nationale (National Security Act), la loi sur la réforme des services de renseignement et la prévention du terrorisme de 2004 et une série de protocoles d'accord et de décrets présidentiels connexes. Selon la législation des États-Unis, les services qui reçoivent les informations sont tenus aux mêmes obligations que le département du Trésor en matière de protection des informations tirées du TFTP. Il convient également de noter que ces informations ne sont échangées avec d'autres agences américaines qu'à des fins de recherche de base, ce qui limite leur utilisation comme preuves déterminantes en justice. Les agences qui reçoivent les informations ont recours à leurs propres bases juridiques pour mener leur enquêtes, y compris pour obtenir auprès d'autres sources des documents susceptibles de servir ultérieurement de preuves en justice.

Ces autres organismes publics échangent également les informations essentielles tirées des données de SWIFT avec leurs homologues étrangers pour les mêmes finalités, moyennant un accord au cas par cas du département du Trésor lorsque cela se justifie pour des raisons de sécurité nationale et de respect des lois. Beaucoup d'informations essentielles tirées du TFTP ont été échangées avec des services étrangers, normalement sans préciser qu'elles émanent du TFTP.

Pour ce qui est d'une éventuelle diffusion publique des données de SWIFT, le département du Trésor traite ces données comme des informations classifiées, sensibles pour le maintien de l'ordre et couvertes par le secret commercial. Par conséquent, il ne les divulgue pas, à moins que cela ne lui soit imposé par la loi, et il s'en tiendra à cette ligne de conduite. À cet égard, pour les procédures administratives ou judiciaires découlant d'une demande d'accès à des données tirées du TFTP introduite par des tiers conformément à la loi sur la liberté de l'information (Freedom of Information Act), le département du Trésor partira du principe que ces informations ne doivent pas être communiquées en vertu de ladite loi.

Recours

Instaurer une procédure de recours dans le cadre du TFTP proprement dit est d'une utilité très limitée en raison du confinement auquel sont soumises les données contenues dans un message de transaction SWIFT, des limitations de l'accès à certaines données SWIFT dans le cadre du TFTP aux fins d'une enquête antiterroriste en cours ainsi que des restrictions imposées en matière de communication d'informations essentielles. Néanmoins, la législation des États-Unis prévoit des voies de recours en cas d'utilisation abusive d'informations par les autorités publiques.

Dans le cas où une personne physique donnée cherche à connaître l'utilisation qui a été faite de certaines informations et les possibilités de recours en cas d'utilisation abusive, il faut opérer une distinction entre les données communiquées par SWIFT et pouvant être consultées et les messages qui sont extraits dans le cadre d'une enquête antiterroriste ciblée et sur la base desquels des décisions administratives ou autres peuvent être prises par les autorités publiques. Les données communiquées par SWIFT en vertu d'une injonction émanant de l'OFAC sont des copies de messages d'opérations financières effectuées, c'est-à-dire des copies électroniques d'historiques d'activités conservés par SWIFT aux États-Unis dans le cadre de l'exercice normal de son activité. Bien que ces données puissent faire l'objet d'un certain traitement aux fins de la recherche très limitée axée sur la lutte antiterroriste qui est décrite ici, il n'est effectué aucune modification, manipulation, adjonction ou suppression de données sur les messages de transactions qui se trouvent dans la base de données interrogeable.

En outre, il est important de souligner à nouveau que, dans leur grande majorité, les messages de transactions communiqués par SWIFT ne seront jamais consultés, même par des analystes en matière de lutte antiterroriste, de sorte que leur contenu n'est pas divulgué. Par conséquent, pour être en mesure de répondre à une demande en matière de protection de la vie privée émanant d'une personne physique souhaitant savoir si des informations le concernant sont conservées dans la base de données, il serait nécessaire, dans la quasi-totalité des cas, de consulter des données qui ne l'auraient pas été dans le cadre du fonctionnement normal du TFTP. Cette consultation contreviendrait au principe établi dans le cadre du TFTP, qui prévoit que toute recherche doit être motivée par un lien préexistant avec le terrorisme. Enfin, les données figurant dans la base de données interrogeable ne pouvant subir aucune modification, manipulation, adjonction ou suppression, il n'y a pas de raison de "rectifier" les informations considérées. D'ailleurs, cela reviendrait à modifier les historiques d'opérations effectuées communiqués en vertu d'injonctions de l'OFAC.

Les données figurant dans un message de transaction particulier ne font l'objet d'un traitement ultérieur que si elles font partie du nombre relativement faible de messages de transactions qui sont extraits de la base de données parce qu'ils répondent aux critères d'une recherche ciblée en matière de lutte antiterroriste. Après extraction de ces données et sous réserve des nombreux contrôles destinés à limiter la communication d'informations dans le cadre de la lutte antiterroriste, les mesures prises par les autorités publiques sur la base des informations ainsi communiquées peuvent faire l'objet d'un recours pour utilisation abusive selon les procédures administratives et judiciaires applicables.

En ce qui concerne les mesures administratives prises par l'OFAC afin de geler des biens en vertu des Global Terrorism Sanctions Regulations mettant en œuvre le décret présidentiel n° 13224, les possibilités de recours peuvent être décrites comme suit: quiconque a été expressément désigné comme étant un terroriste international peut demander que l'OFAC réexamine sa décision par la voie administrative; l'intéressé a alors la possibilité de démontrer que les circonstances ayant mené à sa désignation comme le terrorisme ne sont plus d'actualité et de présenter des arguments et des pièces dont il considère qu'ils démontrent qu'il a été désigné comme tel sur la base d'éléments insuffisants. L'intéressé peut aussi former un recours juridictionnel contre la décision d'une autorité en vertu de la loi sur la procédure administrative (Administrative Procedure Act). Ces voies de recours administratives et juridictionnelles sont accessibles à quiconque fait l'objet d'une décision d'une autorité publique, quelle que soit sa nationalité.

Délais de conservation

Le délai de conservation des informations en rapport avec la lutte contre le terrorisme (ainsi que de toute autre information) est fixé en fonction de nombreux critères clairement définis, y compris les besoins de l'enquête, les délais de prescription et les limites légales applicables en matière de plaintes et de poursuites. L'applicabilité et la mise en œuvre de ces critères, notamment, varient en fonction des tâches et de la mission spécifiques de l'autorité concernée. Par conséquent, les délais de conservation de certains types d'informations en rapport avec la lutte antiterroriste collectées par les différentes autorités dépendent de la nature desdites informations et de l'enquête à laquelle elles sont liées.

Aux États-Unis, les modalités de conservation et d'élimination des documents des autorités publiques sont approuvées par l'agence américaine de conservation des documents administratifs et des archives nationales (National Archives and Records Administration-NARA) en application d'un certain nombre de dispositions législatives et réglementaires. Tous les documents considérés comme d'une utilité limitée dans le temps doivent être détruits au terme d'un délai déterminé fixé en fonction de critères administratifs, fiscaux et juridiques transparents. Parmi les critères retenus par la NARA pour approuver les délais de conservation des documents d'une autorité publique figurent notamment les délais de prescription, les limites légales applicables en matière de plaintes et de poursuites, le risque de fraude, les risques de contentieux et les droits substantiels ainsi que les dispositions législatives et réglementaires accordant ou limitant un droit particulier.

Pour ce qui est des délais de conservation des informations collectées dans le cadre du TFTP, il faut opérer ici aussi une distinction entre les données qui sont communiquées par SWIFT en vertu d'une injonction et les données qui, une fois extraites, servent de base à une décision ou autre mesure administrative des autorités publiques.

Le département du Trésor s'emploiera en permanence, et au minimum sur une base annuelle, à repérer et à effacer toutes les données qui n'auront pas été extraites et qui ne sont pas nécessaires aux fins de l'exécution des tâches mentionnées dans les présentes observations. Sur la base des résultats de cette analyse, toutes les données n'ayant pas été extraites et que le département du Trésor aura reçues de SWIFT après la date de la publication des présentes observations seront effacées au plus tard cinq ans après leur réception. Toujours sur la base des résultats de l'analyse précitée, toute les autres données n'ayant pas été extraites seront effacées au plus tard cinq ans après la publication des présentes observations.

Les données extraites en réponse à une recherche ciblée en matière de terrorisme et ayant été soumises aux nombreux contrôles en matière de communication dans le cadre de la lutte antiterroriste mentionnés plus haut sont conservées pendant la durée applicable à l'autorité publique concernée aux fins des enquêtes dont elle est chargée.

Par exemple, les données SWIFT extraites dans le cadre du TFTP pourraient être exploitées aux fins d'une enquête sur une personne susceptible d'être désignée comme terroriste en vertu des Global Terrorism Sanctions Regulations de l'OFAC. Les modalités de conservation des documents de l'OFAC, qui ont été approuvées par la NARA, prévoient que lorsqu'une décision administrative désignant une personne comme terroriste a été arrêtée à titre définitif (décision qui sera rendue publique), les informations ayant motivé cette décision sont conservées à titre permanent sous forme écrite afin de justifier les mesures prises par l'autorité concernée. Ce dossier de preuves est conservé au cas où la désignation de la personne comme terroriste ferait l'objet d'un recours administratif ou juridictionnel et aussi afin d'alimenter d'autres enquêtes antiterroristes. Par contre, lorsqu'une enquête n'aboutit pas à la désignation de la personne concernée comme terroriste, les dossiers d'enquête sont détruits sur place au plus tard un an après la clôture de l'enquête.

Enfin, conformément au cadre légal en vigueur aux États-Unis et exposé ci-dessus, le délai de conservation des informations essentielles obtenues dans le cadre du TFTP et ayant été divulguées est régi par la réglementation et les modalités applicables au service ou à l'autorité publique destinataire. Par exemple, lorsque de telles informations sont utilisées aux fins de poursuites engagées par le ministère de la justice, elles sont conservées pendant la durée prévue pour ce dernier.

Coopération suivie en matière de lutte contre le terrorisme

Le TFTP a été d'une grande utilité pour la lutte contre le terrorisme dans le monde entier, y compris l'Europe. Le gouvernement des États-Unis continuera d'évaluer attentivement dans quelle mesure les informations obtenues via le TFTP sont de nature à contribuer à la lutte contre le terrorisme et son financement ainsi qu'aux enquêtes, à la prévention et aux poursuites en la matière dans un ou plusieurs États membres de l'Union européenne et il mettra ces informations à la disposition des autorités compétentes chaque fois que cela s'avère opportun et le plus rapidement possible.

En gage de notre détermination à lutter main dans la main avec l'UE contre le terrorisme mondial, une personnalité européenne éminente sera désignée pour vérifier que le programme est mis en œuvre conformément aux présentes observations, dans le but de s'assurer de la protection des données à caractère personnel provenant de l'UE. En particulier, cette personnalité vérifiera que les données non extraites ont effectivement été effacées.

La personnalité désignée devra posséder l'expérience ainsi que l'habilitation de sécurité nécessaires, et elle sera désignée pour une période reconductible de deux ans par la Commission européenne en concertation avec le département du Trésor. Dans l'exécution de ses tâches, la personnalité désignée agira en totale indépendance. Elle ne recevra ni n'acceptera d'instructions de quiconque. Pendant la durée de sa mission, elle s'abstiendra de toute action incompatible avec celle-ci.

La personnalité désignée présentera chaque année à la Commission un rapport écrit sur ses constations et conclusions. La Commission, pour sa part, fera rapport au Parlement européen et au Conseil, selon qu'il conviendra.

Le département du Trésor accordera à la personnalité désignée l'accès nécessaire et lui communiquera les informations et les données requises pour lui permettre de mener à bien sa mission. La personnalité désignée veillera à respecter en toutes circonstances les exigences en matière de secret et de confidentialité fixées par la législation. Les modalités pratiques de ses activités feront l'objet d'un accord avec le département du Trésor.

Le département du Trésor notifiera également à l'Union européenne toute modification importante des garanties énoncées dans les présentes observations et l'adoption de toute disposition législative américaine ayant une incidence sur les indications qui y sont données.

Le département du Trésor s'emploiera à faire publier les présentes observations au Federal Register et consent à leur publication au Journal officiel de l'Union européenne.

_____