# Décision du 9 décembre 2008

**Objet :** Contrôle et procédure de recommandation initiés à l'égard de la société SWIFT scrl

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la LVP), en particulier l'article 30 ;

Vu son Règlement d'ordre intérieur (ci-après ROI), en particulier les articles 37 à 39 ;

Vu la demande de la Commission européenne adressée au gouvernement belge *de s'assurer que la société SWIFT respecte la législation européenne en matière de protection des données à caractère personnel et de prendre les mesures nécessaires à cette fin* ;

Vu le contrôle qu'elle a effectué et les informations qu'elle a recueillies ;

Vu la comparution de la société SWIFT, assistée par Me T. VAN OVERSTRAETEN et Me S. ROUSSEAU, avocats au barreau de Bruxelles, et les mémoires et réponses écrits introduits par ceux-ci ;

Vu la procédure contradictoire ;

Vu le rapport de Monsieur S. VERSCHUERE, vice-président ;

Rend, le 9 décembre 2008, les décisions suivantes :

# I. LA PROCÉDURE

## I.1. LE DÉROULEMENT DE LA PROCÉDURE

1. Lors de sa séance du 23 mai 2007, la Commission de la protection de la vie privée (ci-après la Commission) a décidé d'initier une procédure de recommandation (article 30, § 1er de la LVP) à l'égard de la société SWIFT. SWIFT en a été informée oralement le 24 mai à l'occasion d'une réunion entre ses responsables et le Président de la Commission, et ensuite par courrier du 11 juin 2007. Le Vice-président de la Commission a été désigné en qualité de rapporteur.

2. Dans le cadre de la procédure de recommandation, SWIFT a eu l'occasion de développer et de faire valoir son point de vue conformément à l'article 30, § 2 de la LVP et à l'article 21 du Règlement d'ordre intérieur de la Commission. Les actes suivants ont été accomplis :

- un inventaire des pièces a été dressé pour la procédure de recommandation par le secrétariat de la Commission et a été communiqué à SWIFT le 1er août 2007 ;
- l'avocat de SWIFT a été entendu par le Président le 16 août 2007 ;
- par courrier du 7 septembre 2007, SWIFT a communiqué ses premiers arguments à la Commission et a transmis l'inventaire de son dossier de pièces ;
- SWIFT a été entendue par la Commission lors de la séance du 19 septembre 2007 ;
- après les explications fournies par SWIFT au cours de cette audition, la Commission lui a adressé des questions complémentaires par courrier du 23 octobre 2007, ainsi que le procès-verbal de l'audition. SWIFT a répondu aux questions et a formulé ses remarques sur ce procès-verbal par courrier du 16 novembre 2007;
- lors de sa séance du 19 décembre 2007, la Commission a fixé la suite de la procédure : l'établissement de conclusions provisoires soumises à la contradiction de SWIFT dans un délai de 30 jours et, au cas où SWIFT le souhaiterait, une nouvelle audition pour entendre la société dans ses arguments;
- SWIFT a manifesté le souhait d'être à nouveau entendue après avoir communiqué ses répliques et commentaires aux conclusions provisoires qui lui seraient soumises;
- par courrier du 14 avril 2008 adressé aux avocats de SWIFT, le Président et le rapporteur ont convenu, par préférence et dans la mesure du possible, de fixer le calendrier pour la suite de la procédure de commun accord avec SWIFT après que cette dernière aura reçu les conclusions provisoires, compte tenu que le délai de 30 jours pourrait être prolongé de manière raisonnable si l'un ou l'autre élément le justifiait;
- des conclusions provisoires ont été établies sous la responsabilité du rapporteur et communiquées à SWIFT par courrier électronique et par lettre recommandée à la Poste le 23 avril 2008;

- le 19 mai 2008, le Président et le rapporteur ont tenu une concertation avec les représentants de SWIFT, pour examiner une série de demandes et remarques formulées par cette dernière sur base des conclusions communiquées : **(1)** SWIFT a souhaité accéder à l'ensemble des documents consultés ou obtenus de diverses sources par le secrétariat de la Commission et qui n'avaient pas été exploités à ce stade, afin de s'assurer qu'ils ne contiendraient pas d'éléments que la société estimerait utiles ou nécessaires au débat ; **(2)** en constatant que les conclusions provisoires faisaient appel à des faits jusqu'ici non exploités, SWIFT a estimé que certains de ces faits, bien que décrits sur base des documents en possession de la Commission ou communiqués par la société, étaient établis de manière trop générale, voire imprécise, et que leur exploitation devenait dès lors ambiguë, problématique ou même erronée;
- sur proposition du Président et du rapporteur, la Commission a convenu lors de sa séance du 21 mai 2008 d'ouvrir l'ensemble des documents en sa possession aux avocats mandatés par SWIFT, et de communiquer les pièces pour lesquelles une copie serait demandée, sous réserve d'éléments ou de documents confidentiels qui en tout état de cause ne pouvaient pas être exploités; s'il devait s'avérer qu'un document confidentiel contenait un élément favorable aux positions défendues par SWIFT, le rapporteur et les avocats de la société pourraient s'accorder pour en exploiter la signification manifeste sans en citer la source;
- l'ensemble du dossier du secrétariat de la Commission a été consulté par les avocats de SWIFT les 30 mai et 6 et 11 juin 2008; une copie des pièces réclamées a été fournie; elles constituent le second dossier de pièces de la Commission;
- il a par ailleurs été convenu que SWIFT pourrait apporter des éléments ou informations complémentaires concernant les faits invoqués dans les conclusions provisoires;
- la Commission a fixé le calendrier pour la suite de procédure lors de sa séance du 11 juin 2008, en tenant compte de ces nouveaux développements : **(1)** les réponses écrites aux conclusions définitives établies sous la responsabilité du rapporteur devront parvenir au secrétariat de la Commission au plus tard le 17 septembre 2008 (une version française suffira pour la procédure) ; **(2)** SWIFT sera entendue lors de la séance du 24 septembre 2008 ; **(3)** la Commission prononcera sa décision le mercredi 8 octobre 2008 ; ce prononcé sera précédé d'un débat contradictoire concernant la publication de la décision, dans l'hypothèse où SWIFT formulerait une demande séparée concernant cette question ; si cette éventuelle demande était jointe aux réponses écrites aux conclusions, le débat se tiendra le 24 septembre après le débat sur le fond ; **(4)** les échanges et actes intermédiaires complémentaires devront être accomplis de manière à respecter ce calendrier ;
- SWIFT a été informé de ce calendrier par courrier le 13 juin 2008 ;
- le 25 juin, le rapporteur accompagné de l'administrateur ff. et d'un membre du secrétariat s'est rendu au siège de SWIFT ; il a longuement reçu les explications de différents

responsables de la société ; des documents supplémentaires ont été demandés, que SWIFT a ensuite fournis ;

- le rapporteur a estimé qu'eu égard à la qualité et au nombre des informations recueillies, celles-ci devaient être rigoureusement examinées et précisées pour être intégrées dans un raisonnement cohérent qui en tire les conclusions utiles ; six réunions complémentaires entre les représentants de SWIFT et le rapporteur ont été tenues ; des documents relatifs au contexte (de fait et de droit) du transfert de données personnelles à l'administration américaine du Trésor (UST) ont été recherchés et rassemblés pour constituer le troisième dossier de pièces de la Commission ;
- compte tenu de ces développements, la Commission a donné suite à une demande de SWIFT et a modifié le calendrier de la procédure lors de sa séance du 3 septembre : **(1)** les réponses écrites aux conclusions devront parvenir au secrétariat de la Commission au plus tard le 3 octobre 2008 ; **(2)** SWIFT sera entendue le 8 octobre 2008 ; **(3)** la Commission ouvrira ses délibérations immédiatement après ce dernier débat ;
- les conclusions (définitives) ont été établies sur la base du dossier étayé, sous la responsabilité du rapporteur, et ont été soumises à la contradiction de SWIFT ; elles ont été communiquées à SWIFT par courrier électronique et par lettre recommandée à la Poste le 17 septembre 2008;
- SWIFT a communiqué ses réponses écrites aux conclusions du rapporteur le 3 octobre 2008 et a été entendue le 8 octobre 2008; SWIFT a ensuite communiqué des informations, documents et précisions complémentaires par écrit, le 26 novembre 2008, pour donner suite à certaines questions formulées lors du débat du 8 octobre et confirmer les réponses qui y avaient été apportées;
- lors de sa séance du 26 novembre 2008, la Commission a décidé de clôturer ses délibérations et de rendre sa décision le 9 décembre 2008, étant entendu que SWIFT aura la possibilité de faire valoir son point de vue quant à la publicité de la décision, conformément à l'article 14 du ROI.

## I.2. LES MOTIVATIONS ET LES OBJECTIFS DE LA PROCÉDURE

3. Ayant apprécié les réactions des différents acteurs et intervenants aux avis 37/2006 et 47/2006 de la Commission et 10/2006 ("WP 128") du Groupe 29[1], en ce compris les mesures concrètes adoptées par SWIFT, la Commission a estimé nécessaire d'initier formellement la présente procédure de recommandation dans le cadre du contrôle qu'elle opérait à l'égard de SWIFT conformément à l'article 37 du ROI :

- en considérant que les traitements de données réalisés par SWIFT devaient être examinés au regard des dispositions de la LVP et cela en tenant compte des mesures concrètes adoptées par SWIFT depuis les avis précités de la Commission et du Groupe 29 et, le cas échéant, être encadrés ou accompagnés de recommandations visant à assurer le plein respect de la loi ;
- en considérant la certitude que les autorités européennes exigeraient des autorités belges que celles-ci prennent toutes les dispositions nécessaires pour que SWIFT se conforme aux règles européennes relatives à la protection des données personnelles (exigence notamment confirmée par le courrier adressé par J. FAULL au gouvernement belge le 23 juillet 2007);
- en considérant qu'il était nécessaire de donner suite aux griefs de SWIFT à propos des avis précités ; SWIFT a contesté qu'une qualification juridique puisse lui être attribuée sans qu'elle n'ait pu faire valoir son point de vue devant les instances appelées à se prononcer, alors que cette qualification a pour elle des effets juridiques directs (en terme d'obligations) ou est susceptible de l'affecter de manière significative (notamment son image et sa réputation si des reproches devaient en découler); la procédure de recommandation, contrairement à la procédure d'avis, permet à ceux à qui elle s'adresse d'intervenir;
- en considérant de manière plus générale la nécessité que soient tranchées les questions que SWIFT soulève dans ses griefs, et le besoin manifeste que soient clarifiées les notions de responsable de traitement et de sous-traitant au sens de la LVP, particulièrement lorsqu'il s'agit d'opérations multiples, complexes et entrecroisées réalisées dans le cadre de systèmes permanents de traitements et de transferts d'importants volumes de données personnelles entre de nombreux acteurs et de nombreux Etats[2]; confirmant l'importance d'une clarification, la Banque nationale de Belgique a fait savoir à la Commission, dans un courrier

---

[1] Avis disponible sur le site Internet du Groupe 29 à l'adresse suivante : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf

[2] Cette problématique a été abordée dans de récents bulletins d'information d'avocats, dans la doctrine (voir par exemple TREACY, B., "Current data protection issues for financial institutions- Part I: the 'controller' v 'processor' dilemma. Privacy & Data protection", volume 7, issue 6, 3-6) et dans un atelier de la Chambre de Commerce Internationale consacré à "la distinction entre responsable de traitement et sous-traitant en vertu de la dir. 95/46/CE", sur base notamment du "cas SWIFT" (la Commission a reçu le résumé des différents points de vue exprimés lors de cet atelier).

du 11 septembre 2007, qu'un "facteur d'incertitude au niveau des responsabilités" n'était pas acceptable.

# II. HISTORIQUE

## II.1. LES AVIS DE LA COMMISSION ET DU GROUPE 29

4. Dans ses avis n° 37/2006 du 27 septembre 2006 et n° 47/2006 du 20 décembre 2006[3], la Commission a informé le gouvernement belge de son analyse juridique et de sa position concernant les obligations applicables à SWIFT et aux institutions financières, particulièrement les institutions belges, en vertu de la LVP.

5. La Commission avait alors estimé qu'en ce qui concerne les traitements de données à caractère personnel dans le cadre du service SWIFTNet FIN, SWIFT n'avait pas respecté les obligations qui lui incombaient en vertu de la LVP, en tant que responsable du traitement. Etaient visés le non respect de l'obligation de déclaration, de l'obligation d'information et des limitations de transferts de données à caractère personnel vers des pays non membres de l'Union européenne (articles 17, 9, 21 et 22 de la LVP). Quant à la communication de données à caractère personnel à l'UST (United States Department of the Treasury), la Commission avait estimé que SWIFT aurait dû, dès le début, être consciente et tenir compte du fait qu'outre l'application du droit américain, les règles fondamentales du droit européen de la protection des données devaient être respectées, en particulier le principe de proportionnalité, la limitation de la conservation des données à la durée nécessaire aux exigences du traitement, le principe de transparence, l'exigence d'un contrôle indépendant et l'existence préalable à tout transfert hors de l'Union de normes assurant un niveau de protection adéquat dans le pays de destination. La Commission avait par ailleurs considéré que les autorités compétentes[4] auraient dû être immédiatement informées des demandes de communication formulées par l'UST. Cette information immédiate aurait permis l'élaboration à l'échelle européenne d'une solution compatible avec les exigences du droit européen à la protection des données personnelles, auquel SWIFT restait soumis. Le Groupe 29, qui réunit les autorités nationales de tous les Etats de l'Union, a ensuite exprimé sa position dans un avis du mois de novembre 2006[5]. Cette position était similaire à celle exprimée dans les avis de la Commission, en tout cas pour ce qui concernait la qualification attribuée à SWIFT et l'appréciation des faits et des décisions prises par la société. SWIFT a été informée de ces différents avis.

---

[3] Ces avis sont disponibles sur le site Internet de la Commission à l'adresse http://www.privacycommission.be.

[4] La Commission, ses homologues des autres États membres de l'Union européenne, le Groupe 29 qui réunit les autorités nationales de tous les Etats de l'Union, le Contrôleur européen de la protection des données personnelles (CEPD).et la Commission européenne elle-même en vertu des compétences que lui attribue la dir. 46/95/CE.

[5] Avis disponible sur le site Internet du Groupe 29 à l'adresse suivante :
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf

## II.2. LES FAITS DÉCLENCHEURS, LEURS ANTÉCÉDENTS ET LES SUITES QUI LEUR ONT ÉTÉ RÉSERVÉES

6. Les faits à l'origine des décisions rappelées de la Commission et du Groupe 29 sont, plus indirectement, également à l'origine de la présente procédure de recommandation. Ils ont déjà été exposés dans les décisions précédentes. Il semble toutefois que des faits alors mal connus ou dont l'examen n'est pas apparu manifestement nécessaire, n'ont pas été exposés, exploités ou appréciés à leur juste valeur.

7. Cette constatation suppose une nouvelle description des faits et d'éléments de contexte permettant de les apprécier, particulièrement dans le cadre de la présente procédure et des objectifs qu'elle poursuit.

8. Le 23 juin 2006, le *New-York Times* révélait très largement que la société de droit belge SWIFT, qui exploitait un centre opérationnel basé aux Etats-Unis, aurait collaboré avec la CIA et les agences de renseignement des États-Unis, en leur transférant depuis plus de quatre ans des copies des messages échangés entre les institutions financières du monde entier, dont ces dernières confiaient le transport et l'archivage temporaire aux bons soins de SWIFT. Ce transfert était décrit comme l'élément principal d'un programme gouvernemental secret de surveillance généralisée des transactions financières, dans le cadre de la politique de lutte pour la sécurité des Etats-Unis adoptée par le gouvernement américain et par ailleurs critiquée pour l'étendue des pouvoirs d'exception qu'elle utilisait, sans égard pour les libertés et droits fondamentaux des personnes. L'information a été très largement relayée et commentée par la presse belge et européenne. Un quotidien belge titrait notamment : "Les intrusions de la CIA dans les données confidentielles", et plus tard : "La CIA dicte sa loi en Belgique et en Europe"[6]. Un autre exposait les faits : "*het doorspelen van gegevens van banktransacties aan de Amerikaanse inlichtingendienst CIA*", et titrait peu après, à propos d'un apparent "SWIFT-gate" : "CIA-SWIFT aanslag op privacy"[7].

9. Il est rapidement apparu que SWIFT n'avait pas communiqué de données à la CIA, mais avait transféré des copies de certaines catégories de messages interbancaires, pour des périodes déterminées, à l' "Office of Foreign Assets Control" (OFAC), une division de l'administration du Trésor des États-Unis ("US Department of the Treasury" ou UST). Ces transferts ont été effectués en exécution d'injonctions ("subpoenas") légales et contraignantes adressées par l'UST à la succursale de SWIFT assurant l'exploitation du centre opérationnel américain. Ces injonctions

---

[6] Le Soir, 26 et 28 juin 2006.

[7] De Standaard, 27 et 29 juin 2006.

successives (64 au moment où l'information a été rendue publique) ont été adressées à SWIFT dans le cadre des enquêtes menées aux États-Unis en matière de lutte contre le financement du terrorisme, dont la responsabilité avait été confiée à l'OFAC. Outre les dispositions légales américaines invoquées, les injonctions étaient expressément motivées par l'exécution d'obligations faites aux États par les Résolutions 1333 et 1373 du Conseil de sécurité des Nations-Unies et par les limites que la conformité à ces résolutions imposait.

10. Le 15 octobre 1999, le Conseil de sécurité des Nations-Unies agissant en vertu du Chapitre VII de la Charte des Nations-Unies[8] adoptait sa Résolution 1267, consacrée à la situation en Afghanistan et à la lutte contre les mouvements terroristes agissant à partir du territoire de cet État. Le 19 décembre 2000, le Conseil de sécurité agissant au même titre adoptait sa Résolution 1333, qui confirmait et amplifiait les mesures et dispositifs prévus par la Résolution 1267 et structurait la politique des Nations-Unies en la matière. La Résolution 1333 a ensuite été confirmée de nombreuses fois, et ses dispositifs précisés ou investis de pouvoirs supplémentaires, notamment par les Résolutions 1363 (30 juin 2001), 1378 (14 novembre 2001), 1390 (16 janvier 2002), 1452 (20 décembre 2002), 1526 (30 janvier 2004) et 1805 (20 mars 2008)[9]. Par ses Résolutions 1267 et 1333, ainsi que celles qui les ont suivies, le Conseil de sécurité décidait notamment :

- que "*tous les États devront*" prendre des mesures pour "*geler sans retard les fonds et autres actifs financiers d'Usama bin Laden et des individus et entités qui lui sont associés, tels qu'identifiés par le Comité, y compris l'organisation Al-Qaida, (…) et veiller à ce que ni les fonds et autres ressources financières en question ni tous autres fonds ou ressources financières ne soient mis à la disposition ou utilisés directement ou indirectement au bénéfice*" des personnes et entités visées ;
- de créer, conformément à l'article 28 de son règlement, un comité du Conseil de sécurité, composé de tous les membres du Conseil, et de charger notamment ce comité : de recueillir "*auprès de tous les États des rapports sur les mesures qu'ils auront prises pour donner suite [aux présentes résolutions]"* et *"pour assurer l'application effective des décisions"* du Conseil; d'examiner ces rapports et de rendre compte au Conseil en présentant ses observations et "*des recommandations propres à renforcer l'efficacité desdites mesures*" (Résolutions 1267 et 1333) ; mais encore de "*publier sans tarder les directives et les critères pour faciliter la mise en œuvre des mesures visées*" (Résolution 1390) ; et ensuite, le mandat du comité étant renforcé et étendu, d'assurer, "*outre la supervision de la mise en oeuvre par les États des mesures mentionnées (…), un rôle central dans l'évaluation des renseignements destinés à être examinés par le Conseil en vue de la mise en œuvre*

---

[8] "**Chapitre VII** [de la Charte des Nations-Unies] – Action en cas de menace contre la paix, de rupture de la paix et d'acte d'agression :

**Art. 39.** Le Conseil de sécurité constate l'existence d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression et fait des recommandations ou décide quelles mesures seront prises conformément aux articles 41 et 42 pour maintenir ou rétablir la paix et la sécurité internationales.

(…)

**Art. 41.** Le Conseil de sécurité peut décider quelles mesures n'impliquant pas l'emploi de la force armée doivent être prises pour donner effet à ses décisions et peut inviter les Membres des Nations-Unies à appliquer ces mesures. (…)"

[9] Toutes ces résolutions ont été adoptées à l'unanimité du Conseil.

*effective des mesures, ou de recommander des améliorations auxdites mesures*" (Résolution 1526) ;

- de créer, pour assister le comité, "*un comité d'expert*" (ensuite groupe de suivi) "*chargé de surveiller l'application des mesures énoncées (...) compte tenu des liens qui existent entre les achats d'armes, le financement du terrorisme, le blanchiment de l'argent, les transactions financières et le trafic des drogues*" ainsi qu' "*une équipe d'appui à l'application des sanctions*" composée de 15 membres spécialistes des domaines concernés.

11. Le 28 septembre 2001, le Conseil de sécurité, agissant toujours en vertu du Chapitre VII de la Charte des Nations-Unies, adoptait sa Résolution 1373, relative entre autre à la lutte contre le financement des actes de terrorisme. Cette résolution a été confirmée et précisée à plusieurs reprises, notamment par les Résolutions 1438 (14 octobre 2002), 1440 (24 octobre 2002) et 1450 (13 décembre 2002), et les Résolutions 1526 et 1805 déjà citées[10]. Par sa Résolution 1373, le Conseil de sécurité décidait notamment que tous les États doivent :

- "*prévenir et réprimer le financement des actes de terrorisme*" et "*geler sans attendre les fonds et avoirs financiers ou ressources des personnes qui commettent ou tentent de commettre des actes de terrorisme*" ;
- "*se prêter mutuellement la plus grande assistance lors des enquêtes criminelles et autres procédures portant sur le financement d'actes de terrorisme, y compris l'assistance en vue de l'obtention des éléments de preuve qui seraient en leur possession et qui seraient nécessaires à la procédure*" et "*trouver les moyens d'intensifier et d'accélérer l'échange d'informations opérationnelles*" ;
- "*devenir dès que possible parties (...) à la Convention internationale pour la répression du financement du terrorisme du 9 décembre 1999*".

12. Le Conseil de sécurité décidait également de créer un autre comité du Conseil, composé à nouveau de tous ses membres et chargé de missions similaires à celles du comité des Résolutions 1267 et 1333. Au fil des résolutions successives, la coopération entre ces deux organes subsidiaires officiels a été structurée et amplifiée. Les rapports des deux comités font l'objet de débats périodiques au sein du Conseil de sécurité. Le comité de la résolution 1373 est désormais identifié au niveau international comme le "comité contre le terrorisme" (CCT).

13. De manière générale, les décisions du Conseil de sécurité prises en vertu du Chapitre VII de la Charte s'imposent aux États membres des Nations-Unies et les obligent, et doivent faire l'objet d'une coopération entre eux[11]. Le Conseil de sécurité s'est d'ailleurs systématiquement déclaré

---

[10] Toutes ces résolutions ont été adoptées à l'unanimité du Conseil, à l'exception de la Résolution 1450 (14 voix pour, 1 voix contre).

[11] En vertu notamment des dispositions suivantes de la Charte :

"**Art. 24. 1.** Afin d'assurer l'action rapide et efficace de l'Organisation, ses Membres confèrent au Conseil de sécurité la responsabilité principale du maintien de la paix et de la sécurité internationales et reconnaissent qu'en s'acquittant des devoirs que lui impose cette responsabilité, le Conseil de sécurité agit en leur nom. (...)

"*résolu à prendre toutes les mesures nécessaires pour assurer la pleine application [des présentes résolutions], conformément aux responsabilités qui lui incombent en vertu de la Charte*", ce qu'il a fait au fur et à mesure des résolutions successives, obligeant les États membres de manière de plus en plus précise[12].

14. Le 9 décembre 1999, l'Assemblée générale des Nations-Unies adoptait la Convention internationale pour la répression du financement du terrorisme, ratifiée rapidement par la plupart des États, dont la Belgique et les États membres de l'Union européenne. Cette convention internationale dispose notamment que :

- "*Chaque État partie adopte, conformément aux principes de son droit interne, les mesures nécessaires à l'identification, à la détection, au gel ou à la saisie de tous fonds utilisés ou destinés à être utilisés pour commettre les infractions* [terroristes] *visées à l'article 2*" (article 8.1) ;
- "*Les États parties s'accordent l'entraide judiciaire la plus large possible pour toute enquête ou procédure (…), y compris pour l'obtention des éléments de preuve en leur possession qui sont nécessaires aux fins de la procédure*" (article 12.1) ;
- "*Les États parties coopèrent pour prévenir les infractions visées à l'article 2 en prenant toutes les mesures possibles, (…), notamment : (a) (…) ; (b) des mesures faisant obligation aux institutions financières et aux autres professions intervenant dans les opérations financières d'utiliser les moyens disponibles les plus efficaces (…)*" (article 18.1) ;
- Les États parties coopèrent également "*à la prévention des infractions en envisageant des mesures pour la supervision de tous les organismes de transfert monétaire (…)* " (article 18.2) et en menant "*des enquêtes portant sur les mouvements de fonds en rapport avec la commission de ces infractions*" (article 18.3).

15. Il ne fait aucun doute que les injonctions adressées à SWIFT par l'UST trouvaient un fondement dans les éléments de légalité internationale (incontestés par ailleurs) soulignés ci-avant. Il ne fait aucun doute non plus que les informations recueillies par l'UST lors de la consultation des messages transférés ont été exploitées dans le cadre de la coopération judiciaire et policière internationale visant à lutter contre le financement du terrorisme, imposée aux États par les

---

**Art. 25.** Les Membres de l'Organisation conviennent d'accepter et d'appliquer les décisions du Conseil de sécurité conformément à la présente Charte.

(…)

**Art. 48. 1.** Les mesures nécessaires à l'exécution des décisions du Conseil de sécurité pour le maintien de la paix et de la sécurité internationales sont prises par tous les Membres des Nations Unies ou certains d'entre eux selon l'appréciation du Conseil. **2.** Ces décisions sont exécutées par les Membres des Nations Unies directement et grâce à leur action dans les organismes internationaux dont ils font partie.

**Art. 49.** Les Membres des Nations Unies s'associent pour se prêter mutuellement assistance dans l'exécution des mesures arrêtées par le Conseil de sécurité."

[12] Voir à ce propos J.C. MARTIN, Les règles internationales relatives à la lutte contre le terrorisme, Travaux du CERIC, Bruylant, Bruxelles, 2006, en particulier pp. 421 et ss. : "Pour le première fois de son histoire, [le Conseil de sécurité] définit une infraction internationale *in abstracto* sur le fondement du chapitre VII de la Charte, selon la logique classique du droit international", et la note 409 correspondante : "Les Etats se voient obligés d'incriminer l'infraction internationale dans leur ordre juridique interne et de mettre en œuvre certaines obligations de lutte et de coopération internationale".

résolutions du Conseil de sécurité et la Convention du 9 décembre 1999. Il apparaît d'ailleurs que dans les informations et rapports adressés aux groupes de suivi et équipes d'appui créés par les résolutions du Conseil de sécurité, les Etats-Unis ont indiqué sans réserve la surveillance exercée sur les messages SWIFT disponibles sur le territoire américain et ont inscrit cette surveillance dans les mécanismes coopératifs opérationnels mis sur pied et encadrés par les Nations-Unies. Les comités du Conseil de sécurité ont d'ailleurs apprécié les rapports des États, les ont synthétisé et, dans le cadre de leur mission, en ont tiré des recommandations ou des directives.

16. Ainsi, le Président du Comité créé par la Résolution 1267 transmet tel quel au Président du Conseil de sécurité le troisième rapport de synthèse du groupe de suivi, daté du 4 décembre 2002, le priant de communiquer ce rapport à tous les membres et de le publier comme document officiel du Conseil[13]. Le point 31 du rapport, dans l'exposé de synthèse et le relevé des constatations utiles, souligne :

- "*Le règlement des transactions internationales s'effectue généralement grâce aux relations entre banques correspondantes ou aux systèmes de messages et de paiements concernant des sommes importantes, tels que les systèmes SWIFT, Fedwire ou CHIPS aux Etats-Unis d'Amérique. Ces centres internationaux de compensation jouent un rôle critique dans le traitement des transactions bancaires internationales et sont une mine d'informations sur les paiements. Les États-Unis ont commencé à appliquer de nouvelles techniques de surveillance pour détecter et vérifier les transactions suspectes. Le Groupe recommande que d'autres pays adoptent des mécanismes similaires*."

17. Il convient par ailleurs de rappeler brièvement les justifications données par l'UST aux injonctions adressées à SWIFT et les conditions dans lesquelles le transfert et la consultation de copies de messages ont été effectués :

- SWIFT ne conserve dans son système d'archivage que pendant une période de 124 jours les copies des messages échangés entre les institutions financières ; l'UST a considéré que cette période de conservation était trop courte pour les besoins des enquêtes, à partir du moment où un indice permettait de supposer la présence d'informations utiles dans certains messages échangés à un moment donné, sans que cet indice soit suffisamment détaillé pour permettre dès ce moment-là d'identifier avec précision l'éventuelle transaction suspecte ; l'UST a donc considéré que les messages concernant les périodes suspectes devaient être isolés, copiés et préservés de la destruction afin de pouvoir être exploités utilement sur la base d'informations précises qui seraient recueillies par la suite.
- Après avoir été contrainte de donner suite à une première injonction (émise dans l'urgence directement après les attentats du 11 septembre 2001) concernant des messages

[13] Doc. Cons. séc.ONU du 17 décembre 2002 – S/2002/1338 – disponible sur le site internet du Conseil de sécurité (mention marginale en-tête sur la qualité du document : "Distribution générale").

caractérisés sur la seule base d'une période, et accompagnée d'un engagement que les informations recueillies ne serviraient qu'à la lutte contre le financement du terrorisme (à l'exclusion de toute autre enquête même pénale ou fiscale), SWIFT a formulé des objections aux injonctions suivantes qui présentaient les mêmes caractéristiques, les estimant disproportionnées par rapport à l'objectif poursuivi (eu égard au seul critère de la période, trop peu précis et trop peu motivé; eu égard à l'absence de garantie que les restrictions mises à l'exploitation des informations seraient bien respectées ; eu égard aussi à la fréquence des injonctions suivantes et donc à la quantité d'informations en cause par rapport à l'absence d'encadrement formel et de contrôle).

- Plutôt que de soumettre la question à une juridiction, l'UST a accordé à SWIFT une série de mesures d'encadrement des transferts et de contrôle de l'exploitation des messages concernés. Ces mesures ont été exposées dans les précédents avis de la Commission et seront rappelées infra lorsqu'il s'agira d'en apprécier la portée dans le cadre de la présente procédure. SWIFT a estimé que les garanties obtenues ne permettaient plus de contester la légalité des injonctions devant une juridiction (pour un éventuel défaut de proportionnalité) et a estimé en outre, après analyses et consultations juridiques, que ces garanties étaient supérieures à ce qu'une juridiction aurait pu accorder.
- De manière générale, ces garanties portaient sur : **(1)** une définition stricte du terrorisme reprenant les dispositions pertinentes de droit international ; **(2)** la présentation d'autres indices initiaux, à l'appui de l'injonction, que la seule période dans le temps jusque là invoquée ; **(3)** la consultation des messages obtenus sur base d'indices précis (des noms) et de suspicions légitimées (une information préalable venant d'autres sources) et la limitation de l'extraction et de l'exploitation à ce que ces seuls indices révélaient et aux seules enquêtes antiterroristes ; **(4)** la nécessité que l'information révélée soit confirmée par d'autres sources pour être exploitée (en général par les institutions financières émettrice ou destinataire du message) notamment devant une juridiction ou dans un acte officiel ; **(5)** la mise sur pied d'un audit indépendant, doublé d'un système de **(6)** contrôle permanent de la consultation des messages détenus par l'UST et de la légitimité des indices invoqués et de **(7)** blocage de l'accès aux messages en cas de doute ou de problème.

- **Les observations ("Representations") et les engagements unilatéraux du Département du Trésor des États-Unis**

18. Le 20 juillet 2007, des observations de l'UST ("Representations"), contenant des engagements unilatéraux, ainsi que la réponse de la Commission européenne et du Conseil de l'Union européenne accompagnés d'une déclaration de la délégation française, ont été publiées au Journal officiel de l'Union

européenne[14]. Ces engagements réciproques visent à formaliser et à garantir les conditions auxquelles les injonctions de l'UST à SWIFT doivent désormais répondre et les limites à l'exploitation et à la conservation des données ainsi recueillies par l'administration américaine. Sauf des précisions sur la durée de conservation des messages transférés, les règles ainsi fixées correspondent aux garanties précédemment accordées à SWIFT. Les "Representations" autorisent et prévoient également le contrôle de ces règles par une "eminent European person" indépendante, en plus des audits et contrôles déjà prévus. Cette personne de référence a été désignée, et est assistée par une équipe de collaborateurs. Elle est investie d'un mandat relativement conséquent et détaillé (quant au champ d'investigation qui lui est ouvert et aux pouvoirs qui lui sont attribués).

[14] J.O., volume 50, C 166, p. 17 à 27. Une publication a suivi aux États-Unis le 23 octobre 2007 (Federal Register, Vol. 72, N° 204, p. 60054).

# III. LE POINT DE VUE ET LES ARGUMENTS DE SWIFT

## III.1. LORS DE L'AUDITION DU 17 SEPTEMBRE 2007

19. Dans le cadre de la procédure de recommandation, la société SWIFT a eu l'occasion d'expliquer une première fois son point de vue devant la Commission. Les paragraphes qui suivent synthétisent l'argumentation développée par SWIFT au regard de trois questions:

- le respect des règles régissant les flux transfrontières de données (III.1.)
- le respect de l'obligation d'information (III.2.)
- le respect de l'obligation de déclaration (III.3.)

20. SWIFT considère qu'elle agit en qualité de sous-traitant (au sens de l'article 16 de la LVP) pour ses clients, c'est-à-dire les institutions financières, et ce, tant en ce qui concerne les données personnelles des clients de ces dernières contenues dans les messages transmis via le service SWIFTNet FIN qu'en ce qui concerne les données personnelles transmises en réponse aux injonctions du Trésor américain (UST).

### III.1.1. Quant au respect des règles régissant les flux transfrontières de données (articles 21 et 22 de la LVP)

21. SWIFT indique que, consécutivement à son adhésion au programme de la Sphère de sécurité (Safe Harbor) le 19 juillet 2007, il ne peut plus subsister aucun doute quant au fait que le transfert de données qui lui sont confiées dans le cadre du service SWIFTNet FIN est tout à fait légitime puisque son engagement de respecter les principes du Safe Harbor permet d'assurer un niveau de protection adéquat de ces données dans le cadre de leur transfert aux États-Unis, conformément à la Décision de la Commission européenne 2000/520/CE du 26 juillet 2000. Par conséquent, selon SWIFT, aucune recommandation n'est nécessaire sur ce point.

### III.1.2. Quant au respect de l'obligation d'information (article 9 de la LVP)

22. SWIFT relève que selon l'article 9 de la LVP, c'est au responsable du traitement qu'il incombe d'informer les personnes concernées du traitement de leurs données. SWIFT, en tant que sous-traitant agissant pour le compte de ses clients (les institutions financières) dans le cadre du service SWIFTNet FIN, ne serait donc pas légalement tenue par une telle obligation.

23. SWIFT indique que sans préjudice de ce postulat, elle a mis sur pied deux modes d'information: le premier vise à informer ses clients (les institutions financières), via notamment ses polices, et le second vise à informer le public en général via son site Internet.

24. SWIFT en conclut que l'information détaillée qu'elle fournit à ses clients (les institutions financières) permet à ceux-ci d'informer adéquatement leurs propres clients. Les "polices" et les Questions/Réponses mises en ligne (voir le point II.1.2. et ci-dessous) précisent notamment à cet égard que les institutions financières doivent fournir des informations à leurs propres clients concernant le traitement de leurs données à caractère personnel.

25. *Information sur le site Internet de SWIFT* – SWIFT a rendu accessibles au public sur son site Internet les différentes "polices" mentionnées ci-dessus ainsi que des explications complémentaires sur les injonctions émanant du Trésor américain dans la mesure où ces informations sont publiques. Une liste de Questions/Réponses les plus fréquemment posées (emplacement des centres opérationnels, motif du doublage des données, mesures de sécurité mises en place par SWIFT) a également été publiée sur son site Internet.

26. SWIFT ajoute qu'elle se trouve dans *l'impossibilité pratique* d'informer directement les personnes dont les données sont contenues dans les messages qu'elle transporte pour le compte de ses clients, et ce pour les motifs suivants :

- SWIFT n'est pas en mesure d'informer directement les personnes concernées du traitement de leurs données dès lors qu'elle n'est pas en relation avec ces dernières, contrairement à ses propres clients (institutions financières);

- une information directe des personnes concernées impliquerait pour SWIFT d'ouvrir tous les messages envoyés par ses clients pour vérifier si les messages concernent ou non des personnes physiques et d'en extraire les coordonnées de ces personnes afin de les contacter. À l'heure actuelle, SWIFT ne dispose pas de l'outil nécessaire pour extraire automatiquement les données des personnes dont les données à caractère personnel seraient traitées dans les messages envoyés par ses clients. La mise en place d'un tel outil de recherche impliquerait des coûts de développement significatifs et imposerait à SWIFT de traiter davantage de données personnelles que ce qui est nécessaire pour la fourniture de son service de messages, ce qui serait contraire à la LVP et en contradiction avec les intérêts des personnes concernées.. Une telle procédure serait, à ses yeux, largement disproportionnée au regard de la finalité poursuivie;

- une information directe des personnes concernées serait largement redondante puisque les institutions financières clientes de SWIFT sont déjà outillées pour assurer la communication des informations nécessaires à leurs propres clients étant donné qu'elles sont en contact direct avec ceux-ci.

27. SWIFT relève également qu'une information détaillée concernant la communication de données et leur traitement par le Trésor américain (UST) est contenue dans la lettre adressée à la Commission européenne et au Conseil de l'Union européenne publiée au *Journal officiel* de l'Union européenne. Dans un souci de transparence, SWIFT a inclus un hyperlien vers ces documents sur son site Internet (voir ci-après).

28. SWIFT conclut, au vu de ce qui précède, qu'elle a pris toutes les mesures qui étaient en son pouvoir afin d'assurer une information complète de tous les intervenants, tant en ce qui concerne son service SWIFTNet FIN qu'en ce qui concerne le transfert de données au Trésor américain. Dès lors, aucune recommandation sur ce point n'est nécessaire.

### III.1.3. Quant à l'obligation de déclaration – la qualité de SWIFT (article 17 de la LVP)

29. SWIFT admet ne pas avoir déclaré les traitements de données *opérés dans le cadre de son service SWIFTNet FIN* dès lors qu'à ses yeux, elle agit en qualité de sous-traitant pour le compte de ses clients dans le cadre de ce service. Elle ne serait donc pas tenue d'effectuer une déclaration en application de l'article 17 de la LVP étant donné qu'en vertu de cette disposition, il appartient au seul responsable du traitement de déclarer les traitements qu'il effectue auprès de la Commission de la protection de la vie privée.

30. SWIFT ajoute qu'elle n'est pas plus tenue de déclarer la transmission de données au Trésor américain. Elle a été légalement contrainte de fournir ces données au Trésor américain qui les a requises avec l'objectif de les traiter dans le cadre de la lutte contre le terrorisme. SWIFT n'étant pas intervenue dans la détermination de cette finalité, ni dans celle des moyens mis en œuvre dans le cadre de ce traitement, elle n'est pas davantage tenue de déclarer celui-ci. SWIFT ajoute qu'à cet égard, n'étant pas une institution financière, elle n'est pas soumise à la loi du 11 janvier 1993 *relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux et*

*de financement du terrorisme*. Par conséquent, elle n'était pas non plus tenue de déclarer ces traitements à des fins de "compliance".

31. SWIFT fonde son raisonnement selon lequel elle n'est responsable de traitement ni dans le cadre du service SWIFTNet FIN, ni dans le cadre de la transmission des données au Trésor américain sur les arguments suivants :

- SWIFT ne détermine pas les finalités du traitement :
  *Dans le cadre du service SWIFTNet FIN*, ces finalités – soit, selon les termes de SWIFT, la communication d'instructions de paiement ou d'autres opérations financières sous une forme permettant leur lisibilité par les acteurs concernés, quelle que soit leur localisation géographique - sont déterminées par ses clients, c'est-à-dire les institutions financières.
  SWIFT rappelle à cet égard qu'elle n'a qu'un accès limité au contenu des messages qu'elle véhicule. Elle se limite à vérifier de façon automatisée leur correspondance avec les normes applicables pour assurer une communication lisible entre les institutions financières concernées.

  *Dans le cadre de la communication de données au Trésor américain*, SWIFT argumente que c'est l'autorité américaine et non elle-même qui détermine la finalité de la communication et du traitement des données, soit l'identification d'éléments permettant de lutter contre le terrorisme.

- SWIFT ne détermine pas les moyens du traitement :
  *Dans le cadre du service SWIFTNet FIN*, SWIFT précise d'emblée que la mise en place de son service et son développement (par exemple la mise au point des normes utilisées pour véhiculer les informations nécessaires à l'accomplissement des opérations financières, le principe du doublage des centres opérationnels à des fins de sécurité) ont été pensés par les institutions financières elles-mêmes ou à leur demande de manière à leur permettre de réaliser la communication nécessaire à l'accomplissement d'une opération financière. SWIFT ajoute ensuite que la prise de certaines décisions en ce qui concerne la mise en œuvre et l'architecture de ces services ne lui ôte pas la qualité de sous-traitant. SWIFT invoque à cet égard l'article 16 de la LVP qui n'exclut pas qu'un sous-traitant opère des choix en ce qui concerne les modalités nécessaires - comme les mesures de sécurité - pour exécuter le traitement dans le respect de la loi. De même, la détermination de certains moyens dans le cadre du transport des données confiées par ses clients ne transformerait pas SWIFT en responsable de traitement étant donné l'absence de détermination de finalités dans son chef.

  *Dans le cadre de la communication des données au Trésor américain*, SWIFT souligne que le Trésor américain détermine seul les moyens qu'il entend utiliser pour traiter les données qu'elle est contrainte de lui communiquer.

32. SWIFT défend par contre la thèse selon laquelle elle agit en qualité de sous-traitant pour le compte des institutions financières (clients).

33. Elle s'appuie à cet égard sur la documentation contractuelle relative au service SWIFTNet FIN et à ses différentes "polices", documentation selon laquelle tant sa mission de sous-traitant que le fait qu'elle ne soit autorisée à agir que sur la seule instruction du responsable de traitement sont décrits et reconnus (article 4.5.3. des conditions générales de SWIFT, sections 3.1. et 3.2. de la Personal Data Protection Policy). Dans les faits, le rôle de SWIFT dans le cadre du service SWIFTNet FIN est de transporter des messages pour le compte de ses clients. Les mesures prises par SWIFT sont destinées à assurer la sécurité du traitement qui lui est confié, ce qui est le rôle premier d'un sous-traitant en vertu de l'article 16 de la LVP. SWIFT ajoute également que tant les représentants des banques qui ont participé au groupe de travail au sein duquel les "polices" déjà mentionnées ont été révisées que la Fédération belge du secteur financier (FEBELFIN) au nom des banques belges confirment que SWIFT est un sous-traitant.

34. De façon similaire, le fait que SWIFT ait obtenu des garanties du Trésor américain ne démontrerait en aucune manière qu'elle aurait outrepassé son rôle de sous-traitant. Ce faisant, SWIFT estime s'être conformée à son obligation d'assurer que les données qui lui sont confiées sont traitées dans des conditions de sécurité optimale.

35. SWIFT expose enfin que le service SWIFTNet FIN est un simple service de transport qui ne nécessite en soi aucun traitement de données à caractère personnel.

36. SWIFT ne pourrait toutefois envisager de supprimer les champs mentionnant l'identité des donneurs d'ordre ou des bénéficiaires de paiement dès lors que ces champs résultent d'une obligation imposée par le GAFI (Groupe d'Action Financière), confirmée par le *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*.

37. SWIFT souligne par ailleurs que les autorités nationales de protection des données à caractère personnel ne s'accordent pas sur la qualification de SWIFT. Elle cite en ce sens un avis de l'Agence de protection des données espagnole[15] qui, selon elle, conclut que SWIFT est un sous-traitant agissant pour le compte de ses clients dans le cadre du service SWIFTNet FIN. SWIFT cite également des avis de l'autorité de protection des données du Schleswig-Holstein en Allemagne et de la Commission de protection des données autrichienne[16] aux termes desquels SWIFT aurait été reconnue comme "sous-traitant". SWIFT s'appuie également sur une lettre antérieure à l'adoption de la Directive 95/46/CE (18 juillet 1994) selon laquelle, en réponse à la préoccupation exprimée par la Fédération bancaire de la Communauté européenne au regard de cette problématique, Monsieur R. Vanni d'Archirafi (Direction générale XV) a précisé que le rôle des banques intermédiaires lors d'un transfert nécessaire à l'exécution d'un ordre de paiement pourrait être celui *"d'agents traitants agissant dans le cadre d'un contrat dont l'objet est déterminé et tenues à des obligations de sécurité"*.

38. SWIFT met également en lumière les risques liés à la qualification de responsable du traitement. En qualité de responsable du traitement, SWIFT pourrait se voir contrainte de développer un outil de recherche permettant d'identifier, dans l'ensemble des messages qui lui sont confiés, l'identité des personnes concernées afin de remplir ses obligations quant à la vérification de la qualité et de la proportionnalité des données, à l'information des personnes concernées et à l'organisation de leur droit d'accès. Ce faisant, SWIFT traiterait davantage de données que ce qui lui est nécessaire pour l'exécution de son service de messagerie, contrairement à l'esprit même de la LVP.

39. Enfin, SWIFT entrevoit quelques problèmes pratiques avec ses clients si elle était qualifiée de responsable du traitement :

- dès lors qu'elle n'a pas accès aux données à caractère personnel contenues dans les messages qu'elle transporte, SWIFT ne serait pas en mesure d'assurer le respect de ses obligations en tant que responsable du traitement: SWIFT ne pourrait vérifier que ces données sont adéquates, pertinentes et non excessives au regard de la finalité du traitement (article 5 de la LVP); SWIFT ne pourrait informer individuellement les personnes concernées (article 9 de la LVP) et serait dans l'impossibilité de répondre à une demande d'accès qui lui serait adressée (article 10 de la LVP) ;
- le formulaire-type de déclaration mis à disposition par la Commission sur son site Internet requiert qu'en cas de pluralité de responsables d'un même traitement, comme c'est le cas

---

[15] Agencia espanola de proteccion de datos, Resolucion de archivo de actuaciones, Expediente n° E/00797/2006, 27 julio 2007.

[16] Datenschutzkommission, réf. : K121.245/0009-DSK/2007, 21 mars 2007, Ruling of the Data Protection Commission to SWIFT SCRL.

dans le cadre du service SWIFTNet FIN, la déclaration soit introduite conjointement par tous les responsables.

40. Compte tenu de ces difficultés, SWIFT réclame, à titre subsidiaire, que la Commission indique de façon raisonnable, précise et pratique **(1)** les obligations légales d'un responsable de traitement auxquelles SWIFT devrait se conformer compte tenu des limites susmentionnées et du fait que ces obligations peuvent être assumées par les institutions financières et **(2)** les grandes lignes de la déclaration qu'elle recommanderait.

## III.2. LORS DE L'AUDITION DU 8 OCTOBRE 2008

41. A l'audition du 8 octobre 2008, il a été rappelé que depuis la première audition de SWIFT, de nombreuses réunions ont eu lieu, notamment avec le rapporteur. Des documents non accessibles jusqu'alors ont pu être consultés, une analyse plus approfondie a été menée, laquelle repose sur une meilleure connaissance, compréhension et appréciation des faits.

42. SWIFT a pris acte de ces résultats. Selon la société, les Conclusions du rapporteur sont un tout indissociable de l'ensemble des conséquences juridiques qui y sont décrites, notamment en ce qui concerne les responsabilités et les obligations des différents intervenants à titre individuel et collectif. Si la Commission devait décider de ne pas suivre les Conclusions du rapporteur en tout ou en partie, SWIFT a indiqué qu'elle souhaiterait en être informée pour lui permettre d'examiner et de débattre avec la Commission sur la base de la position développée dans son argumentaire du 7 septembre 2007 et ce, avant que la décision de la Commission ne devienne définitive et a fortiori publique.

### III.2.1. Analyse des Conclusions du rapporteur

#### *(A) Objectif de la procédure et reconnaissance des initiatives de SWIFT*

43. Dans le cadre de la présente procédure de recommandation, dès son premier argumentaire du 7 septembre 2007, SWIFT a souligné le fait qu'elle avait pris toutes les mesures en son pouvoir pour se conformer aux obligations que la Commission entendait mettre à sa charge, tout en continuant à insister sur le fait qu'elle n'y était pas légalement tenue en sa qualité de sous-traitant. Ces mesures sont rappelées par les Conclusions du rapporteur.

44. Compte tenu de ces éléments, Swift a noté que le rapporteur n'a retenu que la déclaration de traitements de données personnelles auprès de la Commission comme formalité unique devant encore être accomplie par SWIFT pour se conformer totalement à la LVP (points 29 et 210 des Conclusions du rapporteur). Le rapporteur précise les circonstances spécifiques dans lesquelles il considère que de telles déclarations sont de mise.

45. En conséquence, SWIFT a indiqué être d'avis qu'il n'est pas pertinent de développer à nouveau un argumentaire en réponse aux allégations de antérieures de la Commission en ce qui concerne le respect de l'obligation d'information et des dispositions relatives au transfert pour lesquelles, autant que de besoin, SWIFT se réfère à son argumentaire du 7 septembre 2007.

#### *(B) Description des traitements de données personnelles dans le cadre des services fournis par SWIFT*

46. Swift a relevé que cinq catégories de traitement ont été identifiées par le rapporteur:
- les traitements effectués par les banques pour leur propre compte;
- les traitements effectués par SWIFT pour le compte de la communauté des utilisateurs de ses services;

- les traitements effectués par SWIFT pour le compte d'un utilisateur spécifique sur requête individuelle (copie de sécurité pour la banque en cas de désastre);
- les traitements effectués par SWIFT pour produire des informations sur les transactions financières;
- les traitements effectués par SWIFT pour répondre aux injonctions contraignantes légalement adressées par elle par une autorité compétente (débat des *subpoenae* américaines).

47. Pour ce qui est des traitements en réponse aux injonctions des autorités, SWIFT a pris acte des Conclusions du rapporteur selon lesquelles la LVP ne leur est pas applicable, tout en contestant que la société puisse être considérée comme responsable de traitement en ce qui les concerne.

### *(C) La finalité des traitements*

48. SWIFT a relevé qu'au terme d'une longue analyse, le rapporteur aboutit à la conclusion que:
- les traitements des 3 premières catégories contribuent à la sûreté des transactions financières par la transmission automatique et sécurisée d'informations standardisées intègres et directement exploitables;
- les traitements de la 4eme catégorie visent la production d'informations générales sur les transactions financières;
- la finalité des traitements relevant de la 5ème catégorie est l'exécution de l'obligation légale (américaine en l'occurrence) à laquelle le responsable du traitement est soumis.

SWIFT a indiqué ne pas partager l'intégralité de l'analyse juridique du rapporteur sur ce dernier point.

### *(D) La qualification des parties intervenantes et la responsabilité des traitements*

SWIFT a résumé de la manière suivante sa compréhension de la qualification des parties intervenantes et la responsabilité des traitements retenues par le rapporteur.

- **Les institutions financières**

49. Lorsqu'elle agit en qualité de banque du donneur d'ordre, de banque destinataire ou encore de banque qui requiert une copie de message, l'institution financière intervient en qualité de responsable de traitement. Cette question ne faisant pas l'objet de la recommandation, elle ne sera pas examinée plus en détail ici.

- **La communauté financière des utilisateurs clients de SWIFT**

50. Le rapporteur a analysé de façon approfondie le processus décisionnel en place au sein de SWIT et de sa communauté d'utilisateurs pour définir qui détermine en définitive les moyens et les finalités du traitement afin d'identifier le responsable de chaque traitement en cause.

51. Le rapporteur a identifié une mutualisation des solutions destinées à satisfaire des besoins communs dont SWIFT est l'expression ultime. Son analyse lui permet de constater une véritable "communauté d'intérêts", tacitement et informellement constituée, et dont les règles collectives de fonctionnement sont établies, mises en oeuvre et respectées depuis plus de trente ans.

52. Le rapporteur en a conclu que SWIFT exprime et matérialise les décisions de cette communauté et agit en étant investi d'une véritable délégation de fait par défaut. Selon le rapporteur, les traitements communs appliqués à tous les messages pour lesquels la communauté financière des utilisateurs clients de SWIFT est responsable sont les suivants:
- décryptage et lecture des messages aux fins d'authentification;
- validation (présence des contenus obligatoires et lisibilité du message) et certification de leur intégrité;

- réencryptage et nouveau décryptage en vue d'un dernier encryptage avec une clé fournie à la banque destinataire;
- duplication et transfert vers le centre de traitement aux Etats-Unis et traitement en miroir de l'ensemble du processus (resilience);
- archivage pendant 124 jours dans les deux centres de traitement;
- destruction des copies archivées après 124 jours.

53. SWIFT a indiqué que cette analyse est confirmée notamment dans l'introduction de son rapport annuel 2007 qui titre "Community inspired" et dispose "*We act as the catalyst that brings the financial community together to work collaboratively to shape the market practice, define standards ans consider solutions to issues of mutual concern and interest*". Cette introduction reflète l'objet social de SWIFT.

- **SWIFT à titre individuel**

54. SWIFT a également rappelé qu'au terme de son analyse, le rapporteur conclut que les seuls traitements pour lesquels SWIFT dispose d'un véritable pouvoir d'appréciation sont ceux que la société réalise sur les données temporairement archivées, à des fins qui ne sont pas directement liées à l'exécution de transactions financières ou à leur sauvegarde. A ce sujet, le rapporteur a fait la distinction suivante:

55. **(1)** Extraction de données et anonymisation en vue de produire des informations, sur les transactions financières : les modalités de traitements de ces données dans ce cadre sont fixées, en consultation avec les utilisateurs, dans ta Data Retrieval Policy laquelle indique que SWIFT ne traite dans ce cadre que des données anonymes. En ce qui concerne ces traitements occasionnels, SWIFT a indiqué qu'elle ne s'opposait pas à une qualification de responsable de traitement.

56. **(2)** Communication de données en réponse à une injonction contraignante : SWIFT a souligné que sur ce point, les Conclusions du rapporteur et la position de la société divergent. SWIFT rejette en effet la qualification de responsable de traitement à l'égard de ces traitements. Elle a soulevé que même si ceux-ci sont envisagés et encadrés par la Data Retrieval Policy, SWIFT n'en détermine ni les finalités ni les moyens.

57. Tout en maintenant sont point de vue selon lequel la qualification de responsable de traitement dans ce contexte n'est pas correcte, SWIFT a noté les conséquences limitées de cette qualification telle qu'elles résultent des Conclusions du rapporteur. Elle a conclu, sans aucune reconnaissance préjudiciable, à l'absence de pertinence de cette qualification dès lors que le rapporteur admet que les données sont transférées aux Etats-Unis et qu'en ce qui concerne les traitements ultérieurs rendus nécessaires à la suite des injonctions du Trésor américain, la LVP n'est pas d'application (avec toutes les conséquences qu'un tel constat entraîne, en ce compris le fait qu'aucune déclaration n'est requise).

### *(E) Les obligations des différents intervenants*

58. SWIFT a rappelé qu'après avoir attribué la responsabilité de chaque traitement, le rapporteur s'est efforcé de décrire de manière pragmatique les obligations à respecter par chacun des intervenants dans le cadre des différents traitements identifiés.

- **Les obligations à charge des institutions financières**

59. Dès lors que la recommandation ne s'adresse pas aux institutions financières, leurs obligations ne sont pas examinées en détail. Chaque banque reste soumise à la loi nationale qui lui est applicable.

- **Les obligations à charge de la communauté des utilisateurs de SWIFT**

60. Selon le rapporteur, SWIFT doit être considérée comme le délégué de fait de la communauté financière de ses utilisateurs clients. SWIFT a relevé que le rapporteur indique expressément que la délégation envisagée est une délégation par défaut. SWIFT ne doit dès lors exécuter les obligations auxquelles la communauté financière est tenue que pour autant que les membres de cette communauté ne soient pas en mesure de les exécuter eux-mêmes.

61. SWIFT a relevé que dès son argumentaire de 2007, elle a indiqué ne pas être en mesure d'exécuter une obligation qui nécessite un contact direct avec les personnes concernées (et notamment une réponse à une demande d'accès aux données par leur titulaire) car elle ne dispose d'aucun moyen pour retrouver les données permettant d'identifier un titulaire dans les messages qu'elle traite. Si SWIFT était tenue de remplir les obligations de la communauté financière sur ce point, elle devrait développer un instrument lui permettant de localiser et de gérer les données identifiantes correspondantes, soit développer un système plus intrusif en termes de protection de la vie privée et des données à caractère personnel que le système actuel. SWIFT a mentionné également qu'un tel système serait assurément rejeté par les banques. Pourquoi, par ailleurs, alors que les banques remplissent déjà ces obligations à titre individuel, les doubler dans le chef de leur délégué?

62. Le rapporteur a passé en revue les différentes obligations à charge de la communauté financière des utilisateurs de SWIFT, en ce compris le transfert de données hors de l'Union européenne, pour arriver à la conclusion que la seule obligation qui, en pratique, n'est pas remplie par les institutions financières de cette communauté serait l'obligation de déclaration des traitements pour lesquels cette communauté est responsable. Le rapporteur a donc proposé que SWIFT effectue cette déclaration pour le compte de cette communauté. SWIFT a préparé un projet de déclaration à cet égard et elle a indiqué être disposée à se conformer à cette formalité au nom de la communauté financière pour autant que la Commission confirme que cette obligation de déclaration est la seule encore à accomplir par SWIFT à ce titre.

- **Les obligations à charge de SWIFT**

63. **(1)** Extraction de_données_et_anonymisation en vue de produire des informations sur les transactions financières : SWIFT a relevé que le rapporteur estime que ces opérations remplissent les conditions pour les traitements ultérieurs fixés par le Roi en vertu de la loi. Le rapporteur précise en outre que le droit d'accès, de rectification et d'opposition n'est pas envisageable concernant des données anonymes. Hormis l'obligation de déclaration, SWIFT en a conclu que, selon le rapporteur, les éventuelles autres obligations de la LVP ont, soit déjà été respectées, soit ne sont tout simplement pas applicables ou bénéficient d'exceptions légales. C'est le cas notamment de l'obligation d'information individualisée qui, en tout état de cause, n'est pas envisageable pour SWIFT dans la mesure où une telle individualisation serait par trop disproportionnée par rapport à l'objectif de protection. SWIFT a également rappelé que dans un souci de transparence, elle a publié des informations générales à cet égard sur son site Internet.

64. **(2)** Communication de données en réponse à une injonction contraignante : SWIFT a souligné que le rapporteur est parvenu à la conclusion que la communication de données au Trésor américain (UST) n'est plus soumise aux obligations de la LVP, du fait même de la qualité de ce transfert. SWIFT n'est dès lors tenue d'aucune obligation de la LVP à cet égard et aucune déclaration ne doit donc plus être effectuée auprès de la CPVP dans ce cadre.

### *(F) Analyse relative à la communication de données au Trésor américain*

65. SWIFT a rappelé que ces communications de données ont été effectuées en exécution d'injonctions légales et contraignantes. Ce faisant, SWIFT a répondu tant à une obligation américaine qu'à une obligation internationale (résolutions des Nations-Unies). SWIFT a rappelé les

protections et garanties obtenues de la part de l'UST, lesquelles ont été confirmées dans les "Représentations" à l'égard de l'Union européenne.

66. SWIFT a indiqué qu'elle ne partage pas l'un des points de droit développés par le rapporteur lorsqu'il considère que les principes de la Sphère de sécurité (Safe Harbor) ne garantissent pas à eux seuls un transfert assurant un niveau de protection adéquat des données et qu'il est nécessaire de les compléter par d'autres garanties, en l'espèce les "Représentations" de l'UST.

67. Selon SWIFT, quid si d'autres autorités exigeaient un accès à ces données en exerçant légalement les pouvoirs contraignants dont elles sont investies ? La réponse à cette question demande une solution politique qui dépasse les pouvoirs de SWIFT et ne ressortit pas non plus de la compétence de la Commission.

68. SWIFT a également réitéré ici son désir de ne pas polémiquer sur les événements passés. Cependant, elle considère qu'il est important de rappeler que la société a tenté de se conformer à la loi alors qu'elle recevait des injonctions dans la foulée des attentats du 11 septembre 2001. Le centre opérationnel installé aux Etats-Unis l'avait par ailleurs été *in tempore non suspecto*. SWIFT apprécierait dès lors que soient éclaircies les suspicions d'infractions dont elle a fait l'objet.

### III.2.2. Position de SWIFT et conclusion

69. En conclusion, SWIFT n'a pas pu souscrire au raisonnement du rapporteur sur deux points: **(1)** la qualité de responsable de traitement en cas de subpoena; **(2)** la nécessaire combinaison des principes du Safe Harbor et des "Représentations" pour satisfaire à l'exigence d'un transfert assurant un niveau de protection adéquat vers les États-Unis.

70. Si SWIFT ne partage pas nécessairement tous les éléments de l'analyse juridique effectuée par le rapporteur, elle reconnaît toutefois l'importance du travail accompli.

71. Compte tenu des avancées, et en espérant que les conséquences décrites dans les Conclusions du rapporteur en ce qui concerne les obligations mises à charge de SWIFT seront confirmées dans leur ensemble par la Commission, la société a lancé les 5 initiatives suivantes:

- préparation avec l'assistance du rapporteur et de son équipe d'une première déclaration en qualité de délégué de fait et par défaut de la communauté financière des utilisateurs de SWIFT;
- préparation avec l'assistance du rapporteur et de son équipe d'une seconde déclaration en qualité de responsable de traitement en ce qui concerne l'extraction et l'anonymisation des données en vue de produire des informations sur les transactions financières;
- réflexion quant au réexamen des "policies" de SWIFT pour déterminer dans quelle mesure celles-ci devraient être modifiées pour tenir compte de la décision de la Commission;
- tenue de réunions périodiques du Data Protection Working Group (DPWG) ;
- participation du Privacy Officer, nommé à temps plein, avec pour mission de superviser le respect de la loi applicable en matière de protection des données dans le cadre des services de la société SWIFT.

72. SWIFT considère que si la Commission devait estimer qu'une recommandation demeurait nécessaire, celle-ci devrait également tenir compte des initiatives précitées et en faire expressément état.

# IV. LA QUALIFICATION DE SWIFT

73. L'avis 37/2006 de la Commission qualifie SWIFT de responsable des traitements de données réalisés via le service SWIFTNet FIN, tout en considérant que les institutions financières exercent également une responsabilité. Selon l'avis 10/2006 du Groupe 29, SWIFT répond à la définition de responsable du traitement tant pour le traitement normal des données à caractère personnel dans le cadre de son service SWIFTNet FIN que pour le traitement assorti d'un transfert de données à caractère personnel à l'UST.[17]

74. SWIFT a contesté cette qualification de responsable de traitement et a déclaré se considérer comme sous-traitant.

75. SWIFT a maintenu sa position quant à sa qualité de sous traitant pendant la procédure de recommandation. SWIFT a toutefois déclaré, en réponse aux conclusions du rapporteur, concevoir l'intérêt des qualifications dégagées par ces conclusions, à l'exception de celle qui concerne les traitements réalisés aux Etats-Unis en réponse aux injonctions de l'UST.

76. La qualification de SWIFT conditionne bien entendu la portée de la présente procédure. La question doit faire l'objet d'un nouvel examen complet, tenant compte **(1)** des arguments de SWIFT, **(2)** d'une connaissance plus approfondie de la situation (du fait notamment des contacts, des échanges et de la collaboration que la Commission a poursuivis avec SWIFT, et des informations transmises par cette dernière, mais aussi d'éléments et informations recueillis parallèlement auprès de différents intervenants lors des recherches et constatations que la Commission a effectuées), et **(3)** d'éventuels faits postérieurs aux avis rendus.

## IV.1. LES SERVICES OFFERTS

77. SWIFT propose à des clients professionnels (principalement des institutions financières) un ensemble de services sous forme de prestations automatisées assurant la transmission sécurisée et surveillée d'informations financières à l'aide de formats standards dont la structure syntaxique est commune à tous les utilisateurs interconnectés, afin de n'accueillir que des contenus lisibles par chaque partenaire.

78. Bien que SWIFT ne soit pas un système d'inscription en compte, de compensation, de transfert de fonds ou de règlement effectif d'une transaction, un nombre croissant de systèmes de

[17] Page 13 de l'avis FR

paiement font appel au réseau SWIFTNet et aux services prestés par SWIFT, d'autant plus que se développent des systèmes de règlement (entre institutions financières) en temps réel. Ces systèmes nécessitent une automatisation performante et sûre de l'ensemble des processus[18], qui s'appuient obligatoirement sur un échange permanent d'informations entre tous les partenaires de la chaîne de paiement.

79. SWIFT définit son réseau "SWIFTNet" dans son glossaire en ligne ("Glossary") comme la *"plateforme de messages avancée basée sur IP. Celle-ci contient un portefeuille de services et de produits qui permettent aux clients de communiquer de manière sûre et fiable des informations financières et des données transactionnelles sensibles"*[19].

80. L'utilisation du réseau SWIFTNet suppose évidemment l'utilisation d'un des quatre services de messagerie proposés par SWIFT (SWIFTNet FIN, InterAct[20], FileAct[21] et Browse). Plus que le réseau lui-même, ce sont ces services de messagerie "génériques" qui contiennent chacun un portefeuille de services spécifiques (par exemple le service FINcopy). Dans son avis n°37/2006, la Commission avait déjà attiré l'attention sur la valeur ajoutée qu'offre le service SWIFTNet FIN, et particulièrement la validation formelle du contenu des messages et leur conservation dans les centres de traitement de SWIFT (service de « back up ») : "*Le service de messagerie comprend, au niveau des centres de traitement, une validation formelle du contenu, notamment la présence ou le contenu correct des données dans les champs prévus (par exemple, la banque de destination est-elle mentionnée ?, la devise est-elle précisée ?, etc.). Cela requiert un décryptage momentané du contenu du message, y compris en ce qui concerne les données à caractère personnel. Ce décryptage a lieu de manière automatisée. En tant que partie du service de messagerie, les messages sont également conservés dans les centres de traitement en Europe et aux États-Unis pour la période susmentionnée de 124 jours.*[22]"

---

[18] Voir la mise à jour du 4 mai 2006 relative à "l'oversight de SWIFT" sur www.swift.com > about SWIFT > Governance > Oversight of SWIFT. Voir également la définition du terme "service" dans les "General Terms & Conditions" de SWIFT, qui fait référence aux prestations des systèmes de compensation et des systèmes de règlement en temps réel et inclut des services de messagerie en faveur de ces systèmes.

[19] "The SWIFT advanced IP-based messaging platform. It comprises a portfolio of services and products that enable customers to communicate mission-critical financial information and transactional data securely and reliably."

[20] Destiné à constituer un environnement pour l'échange de messages en temps réel.

[21] Ce service permet d'échanger n'importe quel fichier ou document via le Réseau SWIFT.

[22] Avis 37/2006, p. 4.

81. Les "General Terms & Conditions" de SWIFT[23] définissent le terme "*service*" comme : "*any value-added service provided by SWIFT (such as the FIN or the Accord or the SWIFTSolutions) or by or for a Service Provider such as a Real Time Gross Settlement, that is accessed by Customers using SWIFT services and products*" (article 1.9). Le glossaire de SWIFT ("Glossary") constitue par ailleurs une liste exhaustive des services offerts par SWIFT à partir des services génériques de messagerie.

82. Le service supplémentaire presté n'ajoute sans doute aucune valeur aux données personnelles elles-mêmes (sauf, dans le cadre du processus d'échange d'information, la valeur d'intégrité que pourra leur attribuer l'institution destinataire du message amenée à son tour à traiter ces données). Le service supplémentaire n'a pas, en tant que tel, pour objet le traitement de ces données personnelles (ce traitement ne serait qu'un effet secondaire inévitable d'une prestation poursuivant d'autres fins). Mais les opérations réalisées sur les données personnelles lors de cette prestation spécifique (dont l'objectif et la plus-value avoués consisteraient à satisfaire les besoins de la communauté financière) restent évidemment soumises aux exigences de la LVP. Il s'agit notamment de garantir les droits et protections des personnes concernées lors de toutes les manipulations des informations qui les concernent.

## IV.2. LES TRAITEMENTS DE DONNÉES : UN EXAMEN DES FAITS

83. L'article 1, § 2 de la LVP définit le traitement comme "*toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel.*"

84. Il convient donc d'identifier les principales opérations qui sont appliquées aux données qui transitent par le réseau SWIFTNet via les services proposés par SWIFT.

85. Afin de déterminer si ces opérations relèvent d'un seul ou plusieurs traitements, il convient d'apprécier si elles poursuivent une seule finalité déterminée ou si plusieurs finalités sont poursuivies.

86. Il convient à cet égard de rappeler que la ou les finalités d'un traitement ne peuvent être confondues avec des objectifs généraux qui correspondraient à l'intérêt individuel ou collectif (les

[23] Dossier de pièces de SWIFT (n° 3.1)

bénéfices et avantages légitimement attendus), au but social ou aux missions légales de ceux qui poursuivent ces objectifs. Mais un traitement de données (dont la portée est circonscrite par sa finalité précise) peut bien entendu participer à la poursuite de ces objectifs généraux[24]. Pour que le traitement soit légal, cette participation doit être nécessaire[25].

87. La finalité d'un traitement doit être déterminée avec précision, sans quoi sa nécessité ne pourrait jamais être attestée. De même, les qualités exigées pour les données traitées ne pourraient jamais être garanties de façon rigoureuse, en telle sorte que les droits des personnes soient effectivement protégés ou qu'ils puissent être effectivement exercés (en particulier l'adéquation, la pertinence et la non excessivité des données, ou encore leur exactitude, qui doivent être garanties au regard des finalités pour lesquelles ces données sont traitées ; ou aussi leur délai de conservation qui ne peut excéder la durée nécessaire à la réalisation de ces finalités)[26].

88. SWIFT décrit l'ensemble des opérations appliquées aux données lors de l'utilisation du réseau SWIFTNet (en particulier dans le cadre du service SWIFTNeT FIN) comme les éléments d'un traitement unique et distinct pour chaque ordre de transfert. Ce traitement (l'opération principale) consisterait en la simple transmission des informations nécessaires aux paiements internationaux concernés et aux transferts de fonds liés, et sa finalité serait la simple exécution des instructions du donneur d'ordre. SWIFT affirme donc limiter l'objet de son intervention à la seule transmission de chacun des messages qui lui sont confiés, et par référence au considérant 47 de la directive 95/46 CE, se décrit comme un prestataire qui se limite à offrir le service de transmission (et n'est donc que le sous-traitant de chacune des banques émettrices pour chacun des ordres qui sont transmis via son service). SWIFT donne à cette prestation limitée une qualité particulière, qui serait assurée au bénéfice des obligations de la banque en tant que supposée responsable du traitement (et mieux que la banque ne pourrait le faire elle-même) et en conformité avec l'obligation faite par la loi à tous les sous-traitants : la sécurisation du traitement de transmission réalisé.

89. Ce raisonnement poussé à l'extrême permettrait de considérer que le véritable responsable du traitement est en fait le donneur d'ordre: la banque elle-même ne ferait qu'exécuter les instructions qui lui sont données par son client. A de nombreux égards d'ailleurs, et plus particulièrement par la jurisprudence, la banque est considérée comme le mandataire de son client

---

[24] Sans qu'il importe pour cela qu'ils aient été déterminés par d'autres que par celui qui traite les données ou même qu'ils présenteraient un caractère d'évidence par rapport à un contexte déterminé Ainsi, la généralisation de l'utilisation de traitements automatisés pour les flux financiers est notamment considérée par la communauté financière comme un objectif inévitable, qui doit nécessairement être atteint dans une société où s'imposent des technologies assurant l'extrême rapidité des échanges auxquels ces flux sont liés, particulièrement les opérations commerciales.

[25] Article 5 de la LVP, en particulier l'al. 1er, e) et f).

[26] Article 4, § 1er de la LVP.

(mandat général pour la conservation et la bonne gestion des sommes confiées; mandats spéciaux pour l'exécution des décisions d'utilisation des fonds: la banque ne peut transférer que les montants déterminés et communiqués par le client; mais celui-ci peut évidemment se tromper). A contrario et sans que cela ne soit contesté, personne n'en a jamais déduit que chacune des opérations (traitements) appliquées aux données de son client par la banque, même en exécution d'un de ses ordres et même si ces opérations sont une conséquence de cet ordre, participerait uniquement à cette exécution et serait effectué dans l'intérêt du client, pour son compte et dans la limite des instructions spécifiques qu'il donnerait à propos de l'opération de traitement de ses données (indépendamment des instructions concernant les mouvements financiers à exécuter), ainsi que l'exigerait la loi si la banque devait être considérée comme mandataire ou "sous-traitant" de son client pour les traitements de données qu'elle effectue.

90. Les considérations générales qui précèdent ne permettent évidemment pas de qualifier l'intervention de SWIFT, quant à son éventuelle responsabilité ou à son rôle de sous-traitant. Elles obligent toutefois à plus de précisions dans la description et l'analyse que SWIFT n'en a proposé dans les premiers arguments qu'elle a avancés.

### IV.2.1. Les opérations réalisées

91. Les données des clients contenues dans les ordres de paiement pour lesquels le réseau SWIFTNet et les services de SWIFT sont utilisés, subissent plusieurs opérations (au sens de la LVP), chacune d'entre elles étant susceptible de relever d'un traitement spécifique ou bien de constituer ensemble avec d'autres opérations un traitement plus général.

92. Les opérations les plus significatives sont les suivantes, étant entendu que l'ampleur de certaines d'entre elles peuvent dépendre du type de relations qu'entretiennent la banque du donneur d'ordre et celle du bénéficiaire, de la plus ou moins grande variété des services de SWIFT utilisés par ces banques et de l'intervention ou non d'institutions ou de systèmes de règlement intermédiaires:

> a) collecte par la banque des données de l'ordre sur la base des informations exigées par les règles spécifiques à l'institution financière, à l'ensemble de ses correspondants, consacrées par les usages bancaires, ou imposées aux institutions financières par les lois et règlements concernant l'exécution d'un ordre de transfert de fonds ;

b) vérification par la banque de l'exactitude des informations recueillies (validation de la réalité des éléments constitutifs de l'opération financière);

c) établissement par la banque du message sur base de structures standardisées exigées par l'utilisation d'une des messageries SWIFT, et contenant des authentificateurs obligatoires (identité de l'émetteur, origine des informations transmises);

d) transfert par la banque des données assemblées vers le réseau SWIFT, soit message par message, soit par lots de messages (qui sont traités individuellement dès leur entrée sur le réseau), après un premier regroupement sur base de critères spécifiques (par exemple, messages non urgents) ou sur base des pratiques de la banque (transferts à heures fixes);

e) toutes les informations contenues dans le message sont signées par le système de la banque (à l'aide d'une clé de signature privée que seule possède la banque, cette clé constituant une paire asymétrique avec une clé publique qui permet uniquement de lire et d'authentifier la signature et dont disposent les autres partenaires de la banque ; SWIFT ne possède que la clé publique de ses clients et utilisateurs)[27] ;

f) premier cryptage des messages par le système de la banque au moment de l'envoi sur le réseau, avec une clé de cryptage déterminée automatiquement par les processeurs de SWIFT[28] sur base d'un "dialogue" avec le système de la banque afin de garantir sa solidité par rapport à l'environnement dans lequel elle sera utilisée (les clés sont donc établies spécifiquement pour chaque institution financière connectée et en fonction de leur système propre ; elles sont modifiées systématiquement plusieurs fois par jour par la même procédure automatisée);

g) accueil du message par celui des deux centres de traitement SWIFT, situés respectivement aux Pays-Bas et aux Etats-Unis, auquel la banque se connecte[29] ;

---

[27] Il ressort des règles de la pratique bancaire que la banque prend la responsabilité du message et de son contenu en le signant.

[28] L'algorithme qui calcule la clé est particulièrement sécurisé, ses performances sont régulièrement auditées et il est réévalué périodiquement.

[29] Les deux centres de traitement sont actifs de la même manière ; les messages peuvent donc arriver indifféremment (pour ce qui est de la suite des opérations) dans l'un ou l'autre centre, en fonction de la ou des connexions de la banque concernée.

h) décryptage et lecture automatisée de chaque message par le processeur régional du système SWIFT[30] attribué à la banque et avec lequel elle est mise en lien (afin de valider le message par rapport à l'existence des données et de la syntaxe requises pour certains champs) ;

i) les signatures liées à toutes les informations sont vérifiées par chaque intervenant lorsqu'il ouvre pour la première fois le message (à l'occasion des décryptages et encryptages successifs), y compris au moment de la réception par le système de la banque destinataire ; cette vérification permet de certifier l'intégrité des données contenues dans le message et leur absolue conformité aux informations collectées au début du processus et intégrées dans le message par la banque du donneur d'ordre[31];

j) transfert du message vers le processeur central SWIFT ("slice processor"), où il est décrypté et encrypté avec une nouvelle clé, interne au système SWIFT;

k) cette centralisation permet ensuite l'orientation et le regroupement de messages destinés à une même institution destinataire ;

l) tant que l'institution destinataire n'est pas connectée au réseau SWIFT, les messages sont maintenus dans une queue d'attente dédicacée par destinataire au sein du processeur central (une duplication des messages est réalisée, les copies étant envoyées et maintenues dans le processeur régional auquel l'institution financière est relié) ; les conditions générales de SWIFT imposent aux utilisateurs du système au moins une connexion quotidienne afin de vider régulièrement les queues d'attente qui se constituent; les processeurs SWIFT conservent toutefois les messages en queue d'attente pendant 14 jours si l'institution destinataire ne se connecte pas ; ce "dépôt surveillé" est destiné à faire face aux "situations de désastre" auxquelles les institutions financières peuvent être

---

[30] Tous les processeurs de SWIFT sont physiquement localisés dans le même centre de traitement ; les différents processeurs régionaux sont les voies d'accès et de dialogue des banques avec le système SWIFT ; ces dernières n'ont pas de connexion directe avec le processeur central ; la répartition des banques entre les différents processeurs régionaux n'est pas fonction de critères géographiques mais de critères propres à SWIFT (types de messagerie utilisée ; sécurisation des accès ; fluidité des l'ensemble des transferts ; prévention des risques de confusion entre institutions présentant des similitudes...).

[31] La validation et la vérification des signatures sont suivies de l'envoi d'un accusé de réception vers l'émetteur (cet accusé de réception est une preuve de prise en charge d'un message correctement formaté et intègre et sa délivrance ou son absence peuvent engager, selon le type de dommage, la responsabilité de SWIFT ou celle de la banque). Les messages non validés ou dont l'intégrité des informations n'est pas garantie font l'objet d'un message d'erreur et de refus de suivi de la part de SWIFT, et sont archivés en l'état (pendant 124 jours).

confrontées et qui imposent une inactivité temporaire (catastrophe naturelle, conflit social, attentat,...) ;[32]

m) dès la connexion de l'institution financière, les messages qui lui sont destinés lui sont envoyés un à un, après avoir été décryptés (abandon de la clé interne à SWIFT) et encryptés à nouveau avec une clé déterminée par SWIFT (et modifiée de la même manière que la clé de l'encryptage initial) qui sera partagée avec le système destinataire;

n) le message sera décrypté par le système destinataire, qui opèrera une dernière vérification des signatures, et le lira automatiquement (avec la certitude qu'il est lisible du fait de la validation syntaxique opérée par SWIFT et la certitude que les informations reçues sont intègres) afin que la banque du destinataire effectue les dernières opérations financières (et les traitements de données qui y sont liés) exécutant l'ordre initial[33] ;

o) le processeur central effectue une duplication des messages et des traitements et le doublage en temps réel de ces derniers ("miroring") dans le centre opérationnel auquel la banque n'est pas connectée, pour pallier les déficiences éventuelles du système, et ensuite en vue du regroupement et de l'archivage temporaire de ces messages pour une période de 124 jours ; les messages sont archivés de la même manière dans les deux centres opérationnels, aux Pays-Bas et aux Etats-Unis ;

p) le message temporairement archivé et sa copie sont détruits définitivement après 124 jours ;

q) les messages validés peuvent être copiés automatiquement et communiqués sur instruction de la banque émettrice à un tiers client de SWIFT qu'elle désigne[34] ; une seule possibilité de copie est offerte[35] ;

---

[32] L'ensemble des processus centralisés au sein des différents processeurs de SWIFT garantit par ailleurs l'uniformité du contrôle, de la qualité du traitement (notamment quant aux temps de transfert et aux règles de réception) et du processus de normalisation qui consacre la "traduction" des messages dans un langage commun assurant l'interopérabilité des systèmes de chaque institution.

[33] A la demande de l'expéditeur, SWIFT peut lui confirmer la délivrance du message.

[34] Cette liberté de choisir ou non l'émission d'une copie et d'en désigner le destinataire peut sembler théorique, et constituer dans la pratique une véritable contrainte lorsque la bonne fin d'une opération de transfert de fonds est régie par un système de règlement interbancaire automatisé en temps réel qui nécessite une telle copie ; cette contrainte n'est toutefois que la conséquence du choix de la banque de participer à l'organisation des marchés financiers de telle ou telle manière ; et à supposer que ce choix-là soit lui-même fort conditionné, il sera avant tout fonction de la nature des marchés financiers dont chaque banque est un acteur, et ne sera pas en tant que tel lié à l'utilisation du système SWIFT.

r) l'ensemble des opérations effectuées est tracé par une numérotation séquentielle propre à chaque message.

93. L'archivage dans une base centrale et commune permet de réaliser les opérations visées par la "Data Retrieval Policy" aux conditions fixées par cette dernière :

s) la récupération et la restitution au bénéfice exclusif et à la demande motivée des clients concernés des données de transfert ou des données contenues dans des messages ;

t) le rapprochement et l'extraction sur base de caractéristiques communes de données de messages différents ou de séries de messages qui ont une origine différente (ne serait-ce que la date puisque celle-ci détermine la durée de conservation) **(1)** pour les agréger sous forme de résultats statistiques et transmettre ensuite à des tiers ces résultats anonymes (sur demande d'organisations collectives afin d'analyser et de comprendre certains aspects des flux financiers), ou **(2)** éventuellement pour répondre aux réquisitions ou injonctions contraignantes légalement adressées par une autorité compétente en vertu du droit applicable et transmettre ces données à l'autorité concernée ;

94. En marge des services commerciaux offerts par SWIFT, des opérations ponctuelles ont effectivement été réalisées par la société sur les messages temporairement archivés en sa possession et les données que ces derniers contenaient, à l'occasion des injonctions de l'UST. Ces opérations sont envisagées et encadrées par la "Data Retrieval Policy" et ont été exécutées dans ce cadre. De manière générale, des situations similaires nécessitant des opérations de même nature pourraient à nouveau se présenter (tant aux Etats-Unis qu'en Europe). L'étendue des opérations et leur particularité seront évidemment fonction de l'étendue, de la particularité et de la force contraignante de l'acte de l'autorité agissante, et des pouvoirs de cette dernière. Mais il semble utile de décrire spécifiquement les opérations effectuées pour donner suite aux injonctions de l'UST afin de pouvoir apprécier ultérieurement la situation et d'en tirer les conclusions utiles. Ces opérations ont consisté en :

u) la sélection, le regroupement et l'extraction de copies de messages archivés sur base de caractéristiques qui leur étaient communes (dans le cas précis des injonctions de l'UST,

---

[35] Les risques de multiplication et de diffusion peu contrôlées des messages et de leur contenu sont de ce fait maîtrisés.

uniquement des dates, le pays d'origine ou de destination et certaines catégories de messages types[36]);

v) la duplication de ces messages et de leur contenu;

w) la communication des copies à l'UST.

95. Deux éléments méritent d'être soulignés et de faire l'objet d'une attention particulière :

- les messages SWIFT sont structurés en deux parties : l'enveloppe et le contenu ; l'enveloppe, à la différence du contenu, ne contient que des données non identifiantes (principalement les coordonnées standardisées de l'institution qui émet le message et celles de la ou des institutions destinataires) et les informations de l'enveloppe sont les seules à être exploitées par SWIFT pour organiser la succession des opérations et l'orientation des messages ; il est certain que SWIFT n'exploite pas les données identifiantes des personnes concernées et ne possède d'ailleurs pas d'outil lui permettant d'accéder directement aux données identifiantes contenues dans les messages qu'elle détient ; les données identifiantes[37] contenues dans les messages font bien l'objet de traitements réalisés par SWIFT (cryptage, décryptage, lecture automatiquement en vue de certifier leur intégrité et de certifier l'intégrité de leur lien avec les données qui les accompagnent, conservation, destruction...), mais ne sont pas exploitées par la société, ni pour l'orientation des messages, ni pour leur regroupement, ni pour leur extraction éventuelle de l'archivage, ni même pour la réalisation de statistiques ;

- les deux centres de traitement de SWIFT sont pleinement actifs ; contrairement à ce qui a pu être affirmé, l'ensemble des données traitées n'est pas initialement concentré dans le centre de traitement des Pays-Bas pour être ensuite transféré vers le centre des Etats-Unis ; les données traitées, qui toutes font l'objet d'un transfert international vers le centre qui ne les a pas accueillies, ont donc, à l'occasion de ce transfert et pour une part d'entre elles, une origine européenne et pour une autre part une origine américaine.

---

[36] Pour le système de messagerie FIN, il y a près de 250 catégories différentes de messages types ; les injonctions de l'UST ne portaient que sur certaines d'entre elles, spécifiquement déterminées et désignées lors de chaque injonction.

[37] Par quoi il faut entendre les données qui identifient directement ou indirectement mais exclusivement la personne concernée, et qui confèrent aux autres informations avec lesquelles elles sont mises en lien le statut de données à caractère personnel : dans les messages SWIFT, il s'agit principalement des nom, adresse, numéro de compte...

96. Il convient enfin de rappeler que la suite donnée à la communication des messages archivés à l'UST était encadrée de manière particulière. Le Conseil d'administration de SWIFT a estimé que la portée des injonctions qui ont suivi celle émise après le 11 septembre 2001 était disproportionnée et qu'elles pouvaient donc être entachées d'un défaut de légalité ; il a avancé à l'égard de l'administration américaine la décision de soumettre la question à une juridiction si ces requêtes étaient maintenues en l'état. Le même conseil a ensuite admis l'obligation de donner suite sans objection et sans recours aux injonctions suivantes, autrement formulées et encadrées, en estimant sur la base d'analyses fouillées n'avoir plus d'argument à faire valoir devant une juridiction concernant la portée excessive et donc la légalité des requêtes.

97. En réponse aux objections initialement formulées par le conseil d'administration de SWIFT, l'UST a fixé les conditions encadrant le transfert, en limitant l'exploitation des données transférées à des traitements qui pouvaient être considérés comme "légitimes" (la lutte contre le financement du terrorisme, ce terme étant bien défini conformément aux conventions internationales, dans un cadre et suivant des procédures légales) et "loyaux" (extraction de données sur base d'indices préalables afin d'éviter une consultation abusive et systématique de toutes les données transférées). Ces conditions ont été consacrées dans un "Memorandum of Understanding" engageant l'administration américaine. SWIFT a par ailleurs obtenu une "comfort letter" de l'administration américaine, à son profit.

98. SWIFT a obtenu le pouvoir de s'assurer que les données transférées ne seraient pas traitées ultérieurement de manière incompatible avec les finalités pour lesquelles elles avaient été transférées. C'est ainsi que bien avant la publication des "Representations" de l'UST, SWIFT a obtenu que des scrutateurs ("scrutinizers") puissent exercer sur place, 24h sur 24h, un contrôle sur la manière dont l'UST traitait les données disponibles aux Etats-Unis. Les "Representations" y font référence en des termes très explicites: *"SWIFT and outside auditors it has retained exercise their independent oversight over the TFTP (Terrorist Finance Tracking Programme) in several mutually complementary ways. First, certain SWIFT representatives have been granted appropriate security clearance to have 24-hour access to the equipment and data and the ability to monitor, in real time and retrospectively, the use of the data to ensure that they are accessed only for counter terrorism purposes. Additionally, these SWIFT representatives may stop any specific search immediately, and even have the ability to shut down the entire system, if they have any concerns"*.

99. En réponse aux objections formulées par SWIFT, l'UST s'est par ailleurs engagée à ce que les informations révélées par les données extraites (sur la base d'indices préalables) ne servent

elles-mêmes que d'indices et fassent l'objet de confirmation par d'autres sources avant d'être exploitées dans une procédure[38].

### IV.2.2. Un moyen essentiel : la standardisation

100. La définition de standards ("SWIFTStandards") et leur utilisation partagée pour l'échange de messages financiers et l'exécution des services associés à l'échange[39], constituent une des caractéristiques essentielles des services que SWIFT propose à l'industrie financière. Le rapport annuel 2007 de SWIFT met en exergue que : "*Standards are the heart of SWIFT's value proposition*".[40]

101. SWIFT décrit ces standards comme "*an agreed way to do things*", et les SWIFTStandards comme "*the overarching name for standards products, tools ans services that SWIFT delivers to the SWIFT Community*"[41]. Ces standards établissent des formats communs et une syntaxe de contenu commune pour l'ensemble des "outils" matérialisant l'exécution des différents services offerts. Ce langage commun ouvre évidemment de nombreuses possibilités d'interaction, d'échanges simplifiés, de validation par une procédure et un intermédiaire uniques, de corrections syntaxiques ou de repérage des fautes syntaxiques par le "maître de la langue" qu'est l'intermédiaire dans le processus de communication.

102. Plusieurs variantes de standards sont utilisées lors de l'échange d'informations via les services de messagerie de SWIFT. Une première variante structure les diverses catégories de messages MT ("Message Type") pour l'utilisation du service FIN. Une autre variante utilise des structures de messages sous un format ouvert (XML). D'autres standards encore ont été développés, dont l'un des impératifs importants était de répondre aux exigences de normes ISO, soit la norme ISO15022, soit la norme ISO20022 (ou norme UNIFI pour "UNIversal Financial Industry message scheme"). Les standards de messages de paiement imposés pour le SEPA (Single Euro Payment Area) en Europe devront être conformes à la norme ISO20022. Lorsque SWIFT traite un message

---

[38] Les plus naturelles de ces sources étant les institutions financières concernées par la transaction, celles-ci étant soumises dans la majorité des États à de strictes obligations d'information et de collaboration avec les autorités en matière de lutte contre le financement du terrorisme. Les confirmations, pour les institutions situées hors des Etats-Unis, nécessitaient donc une collaboration avec les autorités policières ou judiciaires des États concernés (sans pour cela que ces autorités aient été nécessairement ou formellement informées de l'origine de l'information qui leur était transmise).

[39] www.swift.com > Standards.

[40] SWIFT annual report 2007, p. 6.

[41] "Glossary", annexe 3 à la réponse du 16 novembre 2007 aux questions écrites de la Commission.

ISO20022 via son réseau, elle y fait référence comme un message "MX". Les messages MX peuvent être traités via les services FileAct et InterAct.

103. Il convient de relever que SWIFT a été désignée en tant que "ISO Registration Authority" pour l'enregistrement et l'agrément des standards de messages ISO15022 et ISO20022.

### IV.2.3. Les finalités

104. L'examen des opérations rappelées *supra* et de leur contexte, permet de formuler plusieurs remarques concernant la détermination des traitements effectués et de leurs finalités.

105. Il apparaît inexact de décrire la chaîne des opérations comme un seul traitement de transmission propre et distinct pour chaque message. Les informations liées à chaque ordre ne sont pas uniquement l'objet d'une simple transmission par messagerie, mais sont aussi l'objet d'exigences (de forme et de contenu) et d'opérations identiques et communes à tous les messages.

106. Les opérations réalisées sur les données de chaque message ne peuvent non plus être justifiées (ou en tout cas uniquement justifiées) par la nécessité d'assurer la sécurité et la confidentialité des données à caractère personnel que ces messages contiennent lors de leur transfert. On ne peut assurément pas attribuer cet objectif aux opérations réalisées de manière centralisée, qui s'appuient sur l'utilisation indispensable d'un moyen partagé (le langage standardisé commun).

107. A cet égard, il convient de relever qu'à la question: "Pourquoi SWIFT ne peut-elle pas appliquer un cryptage de bout en bout au traitement de données à caractère personnel via son réseau afin de veiller à ce que seules les banques puissent accéder à ces données", SWIFT répond : "*Les clients de SWIFT requièrent le cryptage centralisé. Un cryptage de bout en bout des données empêcherait en effet SWIFT d'effectuer la validation des champs des messages qui est requise de façon centralisée par ses clients. (...) La décentralisation du cryptage impliquerait (...) aussi une remise en question de l'uniformité du système. (...) Les clients de SWIFT ont réitéré leur volonté de maintenir une validation centralisée, cette validation étant considérée comme une caractéristique inhérente et indispensable du service SWIFTNet FIN.*" SWIFT précise encore que la décentralisation du cryptage "*affecterait également la sécurité des opérations dans la mesure où SWIFT ne pourrait*

*plus garantir la sauvegarde de messages dont l'accès serait rendu impossible à la suite de la perte de ses clés d'encryption*."[42]

108. Il apparaît dès lors que la transmission des messages n'est pas le seul objet du service SWIFTNet FIN mais que celui-ci a pour caractéristique essentielle ("inhérente et indispensable") la validation des champs de messages. Le service garantit également "la sécurité des opérations" à un niveau qu'individuellement chaque banque (et donc chaque sous-traitant dans sa relation individuelle avec le responsable qui le commandite) ne pourrait atteindre. Sans même se prononcer sur la qualification de SWIFT, on peut déjà conclure que le considérant 47 de la directive 95/46 CE ne peut manifestement pas être invoqué pour déterminer le statut de SWIFT (cf. *supra* point 88).[43]

109. L'on peut manifestement affirmer que les traitements effectués par SWIFT et par les institutions financières lorsqu'elles utilisent les services de SWIFT afin de contribuer à la poursuite de cet objectif, ont au moins pour finalités précises (liées chacune à une ou plusieurs opérations de traitement) : **(1)** la transmission d'informations financières ; **(2)** l'authentification de la banque émettrice ; **(3)** la certification de l'intégrité des données du message; **(4)** l'assurance de la lisibilité des messages et de l'exploitabilité immédiate des informations qu'ils contiennent pour toutes les institutions concernées (notamment par la validation de la présence d'informations obligatoires dans certains champs et de l'adéquate expression syntaxique) ; **(5)** la communication en temps réel des informations du message validé (par production automatisée de copie) à des opérateurs tiers désignés, par exemple en vue de contribuer à la bonne fin de l'opération (plate-forme de règlement, banque centrale pour l'inscription dans les livres de comptes, institution de règlement…), **(6)** la certification a posteriori et la preuve de l'ensemble des opérations réalisées par les différents intervenants (banque émettrice, SWIFT, banque destinataire) sur chaque message, et **(7)** la compensation des défaillances, notamment celles des systèmes informatiques des institutions financières mais aussi celles qui sont liées à des périodes d'inactivité forcée ou imprévisible de ces institutions (par le traçage, le traitement en miroir, la conservation momentanée en cas de désastre et l'archivage temporaire de 124 jours),...

110. Si un objectif de sécurité existe bel et bien, auquel participent notamment les procédures d'authentification, de validation et de certification, c'est principalement et plus exactement la sûreté des opérations financières elles-mêmes qui est en jeu (la capacité d'exécuter les transactions avec le

---

[42] Réponse de SWIFT du 16 novembre 2007 (point 1.6) aux questions écrites de la Commission.

[43] "*47 – Considérant que lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement des données à caractère personnel contenues dans le message ;* (…)."

moins de risque possible), dans un contexte économique qui implique des relations croisées entre des institutions financières multiples, aux références et règles de fonctionnement parfois fort différentes, et qui exige une rapidité de plus en plus grande voire un traitement immédiat pour ce type d'opérations. Il s'agit notamment de faire correspondre à la rapidité des opérations commerciales, les opérations financières qui en sont le support tout en assurant chaque partenaire que les informations échangées sont compréhensibles, lisibles et intègres (et donc immédiatement exploitables).

111. La standardisation des informations dans un "langage" commun offre la certitude que les ordres croisés des différentes institutions financières pourront être traités de la même manière et dans les mêmes délais et que l'ensemble des institutions financières pourront être interconnectées sur la base de règles d'échange communes et incontestables. Cette double garantie apparaît particulièrement importante alors que les systèmes de règlement en temps réel (*Real Time Gross Settlement*) et l'automatisation de toutes les interventions dans la chaîne de paiement tendent à s'imposer, pour assurer à la fois la rapidité des opérations et la stabilité des marchés[44]. L'interconnexion et la standardisation contrôlée des procédures et des informations sont bien entendu indispensables pour disposer de transferts irrévocables en temps réel[45].

112. Au vu des éléments qui précèdent, il apparaît qu'un des objectifs principaux de SWIFT est de répondre aux besoins collectifs des marchés financiers (rapidité, stabilité, sûreté des opérations financières, harmonisation des échanges,...).

113. C'est dans ce contexte que des autorités financières, et notamment la Banque Nationale de Belgique, ont pu affirmer que l'intervention de SWIFT garantit la stabilité financière mondiale[46]. SWIFT reprend cette affirmation[47].

---

[44] Le fait de pouvoir exécuter immédiatement une transaction financière internationale permet d'éviter le risque de "choc systémique" pour les marchés. Ce risque existe lorsque les transactions entre banques sont simplement inscrites en compte au fur et à mesure de la transmission des informations et que les transferts financiers sont réalisés une fois par jour, à la clôture du compte ; il se peut alors qu'une banque ait donné des ordres de transfert pour des montants supérieurs à ces réserves et ne puisse honorer ses engagements. Le règlement en temps réel permet de s'assurer des réserves de la banque émettrice en permanence, lors de chaque transaction ou série de transactions, et d'augmenter immédiatement les réserves disponibles de la banque destinataire (qui peuvent donc immédiatement couvrir de nouvelles transactions).

[45] Il faut notamment souligner que les mécanismes de règlement pour l'ensemble de la zone euro, TARGET 1 (*Trans European Automated Real Gross Settlement Express Transfer*) et maintenant TARGET 2 sont assurés par l'interconnexion des banques (*Interlinking*) via le réseau SWIFTNet et l'utilisation des services, procédures et standards de SWIFT. Les conditions de cette utilisation sont toutefois externes à SWIFT et sont fixées par les règles et le cadre déterminés par les banques centrales. SWIFT est également mentionnée comme l'intermédiaire de référence sur le site internet du SEPA (*Single Euro Payments Area*) et dans les documents de l'*European Payments Council*.

[46] Voir Rapport de la BNB, "Financial Stability Review", 2005.

114. Une finalité générique à divers traitements de données réalisés par SWIFT ou via l'utilisation des services de SWIFT apparaît manifestement, qui pourrait englober les finalités détaillées plus distinctement au point 109. On pourrait la définir comme : contribuer à la sûreté des transactions financières par la transmission automatisée et sécurisée d'informations standardisées, intègres et directement exploitables[48].

115. De manière non systématique, dans le cadre des requêtes collectives envisagées par la "Data Retrieval Policy", SWIFT procède à l'extraction de données non identifiantes (montants transférés, devises utilisées, dates, origine, destination,...), qui sont dissociées des données identifiantes du message d'origine, et donc complètement anonymisées, pour les regrouper sous forme de valeurs statistiques ou d'informations générales liées à la messagerie financière, à destination d'organismes collectifs et dans le cadre d'études ou d'analyses des marchés financiers. La finalité manifeste dans ce cas peut être définie comme : la production d'informations générales sur les transactions financières.

116. Il importe également de déterminer précisément la ou les finalités des traitements effectués par SWIFT dans le cadre de requêtes ou injonctions légales envisagées par la "Data Retrieval Policy". De manière générale, il faut souligner que SWIFT dispose depuis plus de 15 ans, par cette police, des règles lui permettant de déterminer et de développer une politique spécifique à ce genre de situations, et donc de réaliser d'éventuels traitements de données dans pareil cadre.

117. In abstracto, et en considérant le caractère obligatoire des injonctions et des requêtes qui seraient adressées à SWIFT, faut-il pour autant considérer que la ou les finalités des traitements (réalisés par SWIFT) dans ce cadre se confondraient avec les objectifs poursuivis par les auteurs de l'obligation[49]. Cette hypothèse n'est pas conforme à la LVP, qui distingue bien l'obligation légale, le traitement de données nécessité par cette obligation et la responsabilité de ce traitement. En vérité, il apparaît que ce type d'obligation vise le plus souvent un autre résultat que le traitement lui-même, et que la manière dont elle est exécutée par son destinataire importe peu à son auteur. Ce dernier

---

[47] Dossier de pièces de SWIFT n° 2.2 et 2.3 (document de travail du 7 septembre 2006 et réponse du 7 novembre 2006 à l'avis 37/2006 de la Commission).

[48] Etant entendu que les opérations réalisées par SWIFT ne sont pas suffisantes pour sécuriser les transactions et les marchés et que l'intervention de SWIFT n'a, en tant que telle, aucun effet sur les transactions. Ce sont les partenaires à la transaction qui prennent toutes les décisions ; mais dans l'organisation des marchés internationaux, l'intervention de SWIFT (ou d'un système similaire) leur est nécessaire pour décider. Etant entendu aussi qu'il s'agit de la sûreté de toutes les transactions qui est chaque fois en jeu, et non celle de chacune, séparément : en effet, la sûreté d'une transaction exécutée peut garantir la bonne fin d'un ordre de transfert à venir (cf. note 44).

[49] Cette hypothèse conduirait à désigner sans plus d'examen l'UST comme responsable du ou des traitements effectués.

n'impose pas l'un ou l'autre traitement spécifique, mais un résultat. Et parmi les cinq fondements légaux autorisant un traitement de données à caractère personnel, la loi consacre effectivement le traitement "nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance"[50].

118. Il faut en conclure que la finalité la plus générale que l'on puisse donner à ces traitements, est : l'exécution de l'obligation légale (belge, américaine ou autre selon la qualité de l'auteur et la loi applicable) à laquelle le responsable du traitement est soumis, sans que cela ne donne d'ailleurs plus d'indications sur l'identité de ce responsable (cf. infra – IV.3.4.).

### IV.2.4. La détermination des finalités et des moyens mis en œuvre

119. SWIFT fonde une grande partie de son argumentation sur son absence de pouvoir et de capacité pour déterminer la finalité et les moyens des traitements distincts qu'elle réaliserait pour le compte de chacune des banques clientes sur base des instructions que celles-ci donneraient isolément pour chacun des messages concernés, à savoir le transport du message par la fourniture d'un simple service de messagerie.

#### *(A) La portée de la loi*

120. Pour établir formellement et légalement qui est responsable d'un traitement de données à caractère personnel, il convient effectivement d'identifier celui qui en détermine les finalités et les moyens[51]. Le sous-traitant, par contre, est celui qui traite les données pour le compte du responsable du traitement[52], étant entendu qu'il ne peut agir que sur la seule instruction du responsable du traitement[53].

121. Il en découle logiquement qu'une intervention quelconque pour le compte d'un bénéficiaire instructeur, ne permet pas à celui qui prétend posséder la qualité de sous-traitant au sens de la LVP, de décider d'un traitement de données (opération physique) grâce auquel l'instruction sera exécutée (finalité), ni des moyens à mettre en œuvre pour réaliser cette opération. Le rapport de responsable à sous-traitant se cristallise autour du traitement lui-même, et non d'une opération tierce (serait-elle

---

[50] Article 5, alinéa 1er, c) de la LVP.

[51] Article 1er § 4 de la LVP.

[52] Article 1er, § 5 de la LVP

[53] Article 16, § 1er, 4° de la LVP

un événement nécessaire à l'apparition des données qui seront traitées, et conditionnerait-elle les traitements futurs de ces données-là).

122. Pour établir qui détermine la finalité et les moyens de chaque traitement identifié, il importe donc peu que des institutions ou des groupements (ici les banques, et plus généralement les marchés financiers) aient manifesté un ou plusieurs besoins. La question est de savoir qui décide que ce sera ce traitement particulier-là (opération physique), ayant telle finalité propre, réalisé de telle manière (caractéristiques techniques) et dans telles conditions (moyens généraux, notamment organisationnels) qui satisfera ou concourra à satisfaire ce besoin.

123. La responsabilité d'un traitement suppose au moins une maîtrise (ne serait-ce qu'intellectuelle) de l'ensemble des données traitées ou au moins de l'ensemble des données faisant l'objet d'un traitement automatisé commun susceptible de les rapprocher, et une maîtrise des processus portant sur ces ensembles de données.

- **Les qualifications contractuelles ne sont pas déterminantes**

124. La définition de responsable du traitement à l'article 1, § 4 de la LVP est une disposition légale impérative. Si la désignation d'une partie en tant que responsable de traitement ou sous-traitant dans un contrat peut révéler des informations pertinentes relatives à la qualification juridique de cette partie, cette désignation contractuelle n'est néanmoins pas déterminante pour établir sa qualité réelle. C'est au regard des circonstances concrètes que la qualification doit être réalisée.

125. En outre, le critère de "l'auteur de la collecte" ou de la collecte initiale retenu par SWIFT dans ses polices pour déterminer le processus initial d'une chaîne de traitements qui seraient tous imputables à un même responsable, n'est pas un critère pertinent. Ce critère n'intervient pas dans la définition légale du responsable du traitement. Deux conditions sont exigées pour porter la responsabilité d'un traitement, mais elles sont suffisantes: déterminer les finalités et déterminer les moyens du traitement. La LVP envisage d'ailleurs les cas de traitements de données que le responsable a recueillies indirectement ou qui lui ont été communiquées par le responsable d'un précédent traitement.

- **La notion de sous-traitant a une définition propre en vertu du droit de la protection des données et ne peut être interprétée au départ de sources juridiques externes**

126. La notion de sous-traitant, définie à l'article 1er, § 5 de la LVP, est régulièrement confondue avec la signification courante du terme, telle qu'on peut l'interpréter en dehors de l'application de la

LVP. Certaines institutions financières se réfèrent par exemple à la circulaire PPB 2004/5 de la CBFA qui qualifie explicitement SWIFT de sous-traitant. Cette qualification n'a bien entendu pas été établie en application de la LVP et des critères qu'elle retient, mais en fonction d'autres domaines juridiques qui relèvent de la compétence de la CBFA.

### *(B) Le processus de décision pour ce qui concerne les interventions de SWIFT*

127. SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), est une société coopérative de droit belge, basée à La Hulpe près de Bruxelles. Elle a été fondée en 1973 par 239 banques de 15 pays.

128. Le 30 septembre 2007, SWIFT comptait 8551 clients, les "SWIFT Users" qui ensemble constituent la "SWIFT Community"[54]. Ces 8551 clients se divisent en quatre catégories, les trois premières concernant 7788 institutions financières : **(1)** 2292 coopérants actionnaires ("Members"), **(2)** 3254 filiales ou succursales de ces coopérants actionnaires ("Sub-Members"), **(3)** 2242 membres ne détenant pas d'action ("Non-Shareholding Members") et enfin **(4)** 763 clients qui ne sont ni des actionnaires, ni des institutions financières.

129. Dans l'introduction de son rapport annuel 2007, titré : "Community inspired", SWIFT précise: "*We act as the catalyst that brings the financial community together to work collaboratively to shape market practice, define standards and consider solutions to issues of mutual concern and interest*"[55]. SWIFT affirme à de nombreuses reprises être structurée par une logique communautaire.

130. L'actionnariat de SWIFT est déterminé par l'utilisation des services de messagerie de base que la société fournit. La plus ou moins grande utilisation des services détermine l'importance des parts détenues par chacun des clients (à partir d'un niveau minimal d'utilisation). Les parts sont redistribuées sur cette base tous les trois ans[56].

---

[54] Point 2.8. du questionnaire SWIFT, mentionné en annexe du courrier rédigé au nom de SWIFT en date du 16 novembre 2007.

[55] "Community Inspired", SWIFT Annual Report 2007, p. 1.

[56] "*The Company manages the units through the reallocation principle defined in the by-laws and in the General Membership rules. The units held bye ach member are proportional to the annual contribution paid bye ach member for the network-based services of the Company. The exact number of units allocated toe ach member is determined at least every three years by the Board of Directors, and the members have the obligation to give u por take up the resulting change in units. The by-laws state that units are only reimbursed when a member resigns or when a member has to give up units following a reallocation*". SWIFT Annual Report 2007, p.57

131. La composition du Conseil d'administration de la société exprime également cette logique participative. Le CA est composé de 25 membres. Ils sont nommés pour un terme renouvelable de trois ans sur proposition des groupes de membres nationaux en fonction du nombre de parts détenues par l'ensemble des membres du pays concerné : les actionnaires des six pays détenant le plus de parts proposent collectivement par pays deux administrateurs ; les actionnaires des dix pays suivant proposent collectivement par pays un administrateur ; les autres membres peuvent en s'associant à des membres d'autres pays proposer trois administrateurs.

132. Les administrateurs doivent obligatoirement être issus des institutions financières membres de SWIFT, où ils continuent d'exercer leurs fonctions. Ils ne sont pas rémunérés par SWIFT. L'employeur du Président du conseil d'administration est remboursé de la part salariale correspondant au temps consacré à l'exercice de son mandat[57].

133. Dans sa réponse du 16 novembre 2007 aux questions écrites de la Commission[58], SWIFT détaille ce qu'elle présente comme la structure décisionnelle au sein de la société coopérative. Plusieurs documents précédemment transmis et les informations recueillies par la Commission précisent ce fonctionnement. Les "Corporate Rules" de SWIFT consacrent contractuellement le processus décrit et le rôle des différents acteurs qui y prennent part concernant les décisions opérationnelles importantes[59].

- **Premier niveau : les groupes d'utilisateurs nationaux et les groupes de membres nationaux**

134. Les institutions clientes et éventuellement coopérantes de SWIFT, chacune à titre individuel, sont associées à un groupe d'utilisateurs et, pour les coopérants, à un groupe de membres nationaux. Ces groupes constituent un premier niveau d'examen des problématiques importantes liées aux activités de SWIFT et aux services que la société fournit ou pourrait fournir. Chaque institution est responsable de sa participation ou de sa non-participation à ces groupes. Les "Corporate Rules" de SWIFT précisent que ces groupes d'utilisateurs sont indépendants de la

---

[57] Pour la liste, l'origine nationale et l'appartenance institutionnelle des administrateurs actuels : SWIFT Annual Report 2007, pp. 32-33.

[58] Point 3 de la réponse.du 16 novembre 2007 aux questions écrites de la Commission.

[59] "Corporate Rules" de SWIFT, annexées à la réponse du 16 novembre 2007 aux questions écrites de la Commission (annexe 5). Consultables sur www.swift.com > About SWIFT > Governance > Corporate Rules.

structure juridique et des organes de décision de SWIFT[60]. Ces groupes ne possèdent pas formellement de pouvoir de décision.

135. Les groupes d'utilisateurs nationaux constituent un forum de discussion pour les questions opérationnelles et techniques liées à l'utilisation des services fournis par SWIFT. Ils remplissent également le rôle d'outils d'évaluation et d'indicateurs pour le Conseil d'administration, par le biais desquels la "*communauté des utilisateurs de SWIFT (SWIFT Community) rapporte ses besoins et ses exigences*"[61].

136. Les groupes de membres nationaux sont amenés à se prononcer sur les questions susceptibles d'affecter les membres en cette qualité (conditions d'attribution des parts, valeurs des parts, création de nouvelles catégories d'utilisateurs...). Ils servent aussi "*à coordonner les points de vue des différents membres et à permettre l'adoption de politiques communes*"[62]. Ils présentent les candidats administrateurs, mais on peut dire que, dans les faits, ils les désignent (les membres du conseil d'administration étant répartis par pays – cf. supra). Au demeurant, les membres se prononcent de toute façon en tant qu'associés siégeant au sein de l'assemblée générale.

- **Deuxième niveau : les comités institués par le Conseil d'administration, les groupes de travail *ad hoc* et l'accompagnement du développement technique**

137. Le Conseil d'administration de SWIFT a constitué six comités ("Board Committees")[63] et divers sous-comités chargés de préparer les décisions, afin d'assister les organes auxquels elles seront soumises et qui sont habilités à les adopter. Ce travail préparatoire est notamment destiné à synthétiser et harmoniser les résultats des débats remontant des groupes nationaux[64].

138. Deux groupes de travail *ad hoc* ont été créés par le Conseil d'administration. Un premier groupe de travail, appelé le "Data Privacy Working Group" ou "DPWG", a été créé en décembre 2006. Il avait pour mission de formuler des propositions pour répondre aux griefs formulés par la

---

[60] Articles 3.4 et 3.5. des "Corporate Rules" : "The National [User or Member] Group is independent from the SWIFT legal and governance structure and can organise as it thinks appropriate"

[61] Point 3 du questionnaire SWIFT, mentionné dans l'annexe du courrier rédigé au nom de SWIFT en date du 16 novembre 2007.

[62] Point 3 (Introduction) de la réponse du 16 novembre 2007 aux questions écrites de la Commission.

[63] Les comités cités comme pertinents au nom de SWIFT sont le "Technology & Production Committee", le "Standards Committee" et les "Banking & Payments/Securities Committees".

[64] Points 1.7. in fine, 2.1. et 3 du questionnaire SWIFT, mentionné dans l'annexe du courrier rédigé au nom de SWIFT en date du 16 novembre 2007.

Commission et par le Groupe 29, et en particulier d'émettre des propositions en ce qui concerne l'adhésion au Safe Harbor. Un second groupe de travail a, quant à lui, été chargé de proposer des adaptations à l'architecture de SWIFT (la "Re-architecture Board Task Force" ou "RBTF"). Ces groupes ont été majoritairement composés de "représentants de la communauté financière".

139. Plus spécifiquement, pour ce qui concerne le développement de standards et de processus techniques, une série d'étapes et d'interventions sont clairement identifiables :

- identification d'un besoin collectif, en général par une manifestation quelconque d'un ou plusieurs utilisateurs ou de catégories d'utilisateurs ;

- définition précise des impératifs à rencontrer et des solutions techniques pour satisfaire le besoin (business model and logical model) ; les *business* et *logical models* sont développés par SWIFT avec l'accompagnement d'un "modelling group" composé d'experts techniques du domaine particulier pour lequel le projet de standard est développé ; ce travail est lui-même accompagné et validé par un "business validation group" également composé d'experts des institutions financières ;

- présentation du projet à l'ensemble des utilisateurs clients, qui s'expriment notamment via un vote (dont le résultat est rapporté vers SWIFT par pays, et pondéré en fonction des votes positifs et négatifs exprimés au sein des groupes nationaux) en vue d'apprécier la plus ou moins grande adhésion suscitée par le projet ;

- poursuite éventuelle du développement du projet s'il apparaît que le plus grand consensus n'est pas atteint ;

- prise de décision formelle sur la base de la constatation que le plus grand consensus de l'ensemble des utilisateurs clients est atteint.

140. Les dispositions contractuelles les plus importantes figurant dans les polices de SWIFT sont élaborées suivant des procédures similaires.

- **La prise de décision**

141. C'est le conseil d'administration qui prend les décisions proprement dites concernant les développements techniques et les dispositions contractuelles des polices. Mais il est indéniable que ces décisions procèdent d'une logique communautaire et que, tel que le fonctionnement de la

société a pu être observé par la Commission, il n'y a pas de décision qui irait ou serait allée à l'encontre du plus grand consensus communautaire.

142. Il s'agit plus que d'une simple consultation de la clientèle (ce qui relèverait au demeurant de la bonne logique commerciale), dès lors que la clientèle contrôle aussi les organes de la société de sorte à garantir que ses volontés qui se sont exprimées dans des structures externes et indépendantes sont bien respectées et exécutées. Pour ce type de décisions, c'est la clientèle qui s'exprime mais c'est aussi véritablement elle qui décide, de manière collective.

143. On peut affirmer qu'il s'agit d'une opération de mutualisation des solutions destinées à satisfaire des besoins communs. La société SWIFT est l'expression ultime de cette opération. Mais elle n'en est pas le seul vecteur, ni le seul instrument. Ce n'est pas SWIFT qui matérialise l'existence de la communauté financière et qui dès lors la constituerait[65]. SWIFT n'est pas la communauté financière de ses utilisateurs clients[66].

144. Il n'existe pas d'acte constitutif de cette communauté. Mais les faits décrits permettent de constater l'existence d'une véritable communauté d'intérêt, tacitement et informellement constituée, active et dont les règles collectives de fonctionnement sont établies, mises en oeuvre et respectées depuis plus de 30 ans.

145. Si cette communauté d'intérêt n'est pas formellement constituée, il y a toutefois parmi les éléments qui attestent son existence, des instruments juridiques de droit belge (et uniquement de droit belge):

- les règles de fonctionnement de SWIFT et les actes internes qui organisent le processus décisionnel et sanctionnent son résultat, en application de ces règles ;
- les différentes polices contractuelles de SWIFT, dont certaines dispositions consacrent le processus décisionnel décrit mais qui sont surtout communes à tous les utilisateurs de SWIFT.

146. Il est significatif (autant qu'exceptionnel) que certaines règles organisant la prise de décision des grandes orientations et réalisations de SWIFT soient établies et consacrées par des dispositions contractuelles liant la société à ces utilisateurs clients[67].

---

[65] Même dans la limite d'une communauté qui ne serait constituée que dans le seul objectif de mettre en commun les besoins auxquels SWIFT répond.

[66] Comme on l'a montré, la communauté et ses membres ne s'expriment et ne décident pas au sein d'un organe de la société qui les regrouperait à cette fin (par hypothèse, l'assemblée générale).

[67] En particulier les "Corporate Rules"

147. Il est difficile de considérer SWIFT comme une entité indépendante de la communauté de ses utilisateurs, dans la mesure où la société a été créée au sein de cette dernière, que l'utilisation des services de SWIFT est la voie pour y adhérer et que SWIFT exprime la volonté collective. SWIFT n'existerait pas sans la communauté de ses utilisateurs. Mais cette communauté, en cette qualité, n'existerait pas sans SWIFT.

148. Sans disposer des mêmes prérogatives que les institutions financières qui constituent la communauté des utilisateurs de la société, SWIFT peut être considéré comme une entité liée par essence à la communauté, dotée d'un statut spécifique et de pouvoirs limités mais clairement déterminés.

149. En vérité, SWIFT, à l'intervention de ses organes, est le garant, le greffier et l'exécuteur des décisions de la communauté financière qui s'est réunie autour d'enjeux et de besoins communs. On peut considérer que SWIFT exprime et matérialise les décisions de cette communauté, et agit en étant investi d'une véritable délégation de fait.

150. Par ailleurs, il apparaît clairement qu'un ou plusieurs clients de SWIFT ne pourraient pas imposer de solutions ou d'exigences particulières jugées marginales par la communauté des utilisateurs. SWIFT n'élabore pas et n'a pas pour mission d'élaborer, à la demande, de solution "sur mesure" pour quelques clients. Mais rien n'empêcherait ces clients de faire élaborer ces solutions par ailleurs : "l'appartenance communautaire" n'est pas exclusive, pas plus qu'elle n'est définitive ; elle ne suppose pas l'abandon de l'indépendance de chacun des membres de la communauté.

151. Il convient enfin d'indiquer que certaines décisions prises par le Conseil d'administration de SWIFT, et qui impliquent des traitements de données personnelles, ne font pas l'objet du large processus collectif et communautaire de décision. Il s'agit des décisions prises dans le cadre des dispositions de la "Data retrieval policy" pour ce qui concerne l'extraction et l'agrégation à des fins statistiques et pour ce qui concerne l'extraction et la communication suite à des requêtes ou injonctions légales d'autorités publiques. Ces décisions font chaque fois l'objet d'une appréciation du conseil d'administration et peuvent nécessiter le développement d'outils techniques spécifiques permettant de les exécuter[68].

---

[68] Les décisions d'extraire de l'archivage temporaire et de communiquer au client concerné, à sa demande et à son bénéfice, la copie d'un message dont il était l'expéditeur ou l'un des destinataires ne peuvent par contre faire l'objet que d'une appréciation très marginale, qui consiste à vérifier que la demande correspond bien aux situations spécifiques dans lesquelles seraient placés les demandeurs et qui sont décrites dans la "Data Retrieval Policy" ; la détermination de ces situations a fait l'objet du large processus de concertation de la communauté financière des utilisateurs clients.

### *(C) Le rôle central de SWIFT et l'autonomie des banques*

152. L'utilisation des services SWIFT semble difficilement évitable pour certaines opérations financières : envoi de messages internationaux relatifs à des transactions à caractère urgent, de grande valeur et ayant un potentiel de risque élevé ; transmission d'informations financières dans le cadre d'une transaction qui s'accompagne d'un règlement automatisé en temps réel.

153. Il apparaît d'ailleurs que l'intervention de SWIFT ne s'effectue pas simplement pour le compte du donneur d'ordre ou de sa banque, mais que les traitements réalisés par SWIFT sont aussi réalisés au bénéfice du destinataire (et donc pour son compte, dès lors qu'il donne effet à l'authentification, la certification et la validation réalisées par SWIFT), et également au bénéfice de la communauté financière dans son ensemble (et de tous ceux qui ont un intérêt à la stabilité des marchés financiers).

154. SWIFT assume et revendique ce rôle de tiers de confiance ou de tiers certificateur entre les partenaires d'une opération financière.

155. L'importance des services et de l'intervention de SWIFT dans ces marchés est confirmée par SWIFT et la Banque nationale de Belgique[69] lorsqu'elles affirment que SWIFT a été mise sous la surveillance des banques centrales du G10 en raison de son "*importance critique pour le bon fonctionnement du système financier global, dans son rôle de fournisseur dominant de messageries et de services de traitement, en particulier pour l'acquittement de paiement et les transactions de titres.*"

156. On ne peut toutefois déduire de cette situation que les banques, individuellement, auraient perdu toute autonomie et seraient nécessairement soumises à une sorte de monopole qu'exercerait SWIFT et qui les priverait de tout pouvoir de décision. En vérité, ce n'est pas un "monopole" de SWIFT qui conduirait les banques à utiliser les services prestés par la société mais plutôt la nature même des opérations financières internationales entre plusieurs partenaires, et la nécessité de règles communes entre un maximum d'entre eux (dès lors que les effets financiers de chaque

---

[69] BNB, Financial Stability review 2005 (page 13) : "*Toutefois, en raison de l'importance systémique de SWIFT pour le système global des paiements, les banques centrales du Groupe des Dix (G10) ont estimé que SWIFT devait faire l'objet d'une surveillance concertée entre banques centrales.*" Ce document est disponible à l'adresse http://www.bnb.be/doc/ts/Publications/FSR/FSR_2005_FR.pdf

opération financière se cumulent ou s'influencent, même si individuellement elles concernent chacune des partenaires différents).

157. L'utilisation des services de SWIFT n'est pas obligatoire, et relève de la décision de la banque de s'intégrer ou non dans la dynamique de marché mise sur pied par les utilisateurs clients de SWIFT. Les institutions bancaires restent par ailleurs libres de choisir la manière dont les ordres de paiement internationaux sont effectués, sous réserve de l'accord de l'institution financière partenaire à l'opération. L'institution bancaire peut décider de faire circuler les données via son propre réseau (transactions "on-us" internationale entre deux banques du même groupe), éventuellement via un VPN[70], via un autre prestataire de services financiers (traitements via SIANet, BT/Radianz, VISA, Mastercard,...) ou via un simple opérateur de télécommunications (par fax, par mail...).

## IV.3. LA RESPONSABILITÉ DES TRAITEMENTS RÉALISÉS PAR SWIFT

### Des qualifications et des responsabilités distinctes pour les différents traitements de données personnelles effectués à l'occasion de la transmission d'informations financières via les services de SWIFT

158. La constatation et la description des faits permettent de désigner plus sûrement les responsables des différents traitements réalisés. Pour cela, il faut bien entendu apprécier le fait que le responsable doit garder la maîtrise, ne serait-ce qu'intellectuelle, tant du traitement que des données traitées, et que le traitement ne peut évidemment dépasser ce que le responsable présumé est capable de maîtriser ou ce que théoriquement il aurait été capable de réaliser, à supposer qu'il ait eu les moyens de le faire ou qu'il ait choisi de mobiliser ces moyens.

### IV.3.1. La responsabilité de chaque institution financière

159. La banque de chaque donneur d'ordre doit être considérée comme responsable de traitement (et titulaire des obligations liées) là où les aspects individuels et propres à chaque ordre dominent : collecte des données (et vérification de leur exactitude) ; établissement du message conformément aux structures standardisées, aux obligations légales et aux instructions du donneur d'ordre ; transfert vers le réseau SWIFT ; premier cryptage (dont la clé est établie par SWIFT, mais sur base du système de la banque, et qui est effectué par le système de la banque) ; transfert de

[70] Virtual Private Network.

copies du message, par exemple vers une plate-forme de règlement automatisé ; transfert des informations du message vers la banque du destinataire.

160. Il faut d'ailleurs constater que le Règlement CE 1781/2006 du 15 novembre 2006 "relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds" oblige le prestataire de services financiers du donneur d'ordre de s'assurer de l'identité de ce dernier, d'accompagner l'ordre de transfert de fonds de données permettant son identification et de conserver ces données pendant cinq ans. A considérer l'article 1er, § 4 al. 2 de la LVP, ces dispositions désignent manifestement la banque du donneur d'ordre comme responsable de ces différents traitements[71]. Les prestataires de services de messagerie sont d'ailleurs clairement exclus du champ d'application de ce Règlement[72].

161. En outre, la création de files d'attente propres à chaque banque destinataire relève des décisions de chacune de ces banques (temps et périodes de connexion au réseau SWIFT). Ces files d'attente, ainsi que le dernier décryptage et les traitements ultérieurs des données des messages destinés à faire aboutir l'opération financière, relèvent manifestement de la responsabilité de la banque destinataire.

162. Enfin, il faut considérer que l'extraction et la production d'une copie d'un message archivé à la demande de son expéditeur ou d'un de ses destinataires relève manifestement de la responsabilité du demandeur, dans la mesure où le système d'archivage a été conçu dans le but de produire des copies de sauvegarde pour les demandeurs potentiels en cas de besoin, qu'il s'agit de messages dont les demandeurs ont déjà eu connaissance, qu'ils ont la capacité d'accéder eux-mêmes à l'archivage pour récupérer directement leurs messages et que l'intervention de SWIFT se limite à pallier les déficiences éventuelles du système d'une institution lorsqu'elle tente d'accéder aux messages archivés qu'elle peut récupérer.

---

[71] "Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'un ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance".

[72] Voir considérant (8) du Règlement CE 1781/2006.

### IV.3.2. La responsabilité de la communauté financière des utilisateurs clients de SWIFT

163. La communauté financière des utilisateurs clients de SWIFT peut manifestement être considérée comme responsable des traitements communs appliqués à tous les messages (ou à chaque catégorie de messages selon le service utilisé) qui transitent par le réseau SWIFTNet.

164. Plus précisément, la communauté financière des utilisateurs clients de SWIFT peut être considérée comme responsable des traitements suivants : décryptage et lecture des messages aux fins d'authentification, validation (présence des contenus obligatoires et de la lisibilité du message) et certification de leur intégrité ; réencryptage (avec une clé interne) et nouveau décryptage en vue d'un dernier encryptage avec une clé fournie à la banque destinataire ; duplication et transfert vers le centre de traitement aux Etats-Unis et traitement en miroir de l'ensemble du processus ; archivage pendant 124 jours dans les deux centres de traitement ; destruction des copies archivées après 124 jours.

### IV.3.3. La responsabilité de la société SWIFT

165. La société SWIFT, en tant que telle, peut manifestement être considérée comme la responsable des traitements que, sur base de sollicitations particulières, elle réalise sur les données ou une partie des données temporairement archivées, à des fins qui ne sont pas directement liées à l'exécution de transactions financières : la sélection, le rapprochement et l'extraction sur base de caractéristiques communes de données de messages différents ou de séries de messages qui ont une origine différente, pour les agréger sous forme de résultats statistiques et transmettre ensuite à des tiers ces résultats anonymes (sur demande d'organisations collectives afin d'analyser et de comprendre certains aspects des flux financiers). Il importe de souligner que le système d'archivage n'a pas été conçu pour répondre à de telles demandes. L'opportunité que représente l'archivage et qui rend possible ces derniers traitements, confère à SWIFT une responsabilité marginale mais complète et autonome, consacrée par un véritable pouvoir d'appréciation.

### IV.3.4. Les cas spécifiques des traitements réalisés pour donner suite à une injonction administrative ou judiciaire contraignante

- **l'impossibilité d'une qualification "générique" et la nécessité d'une qualification fondée sur une appréciation in casu de chaque situation**

166. Les injonctions et requêtes administratives ou judiciaires contraignantes peuvent être de nature et de contenu très différents, selon l'étendue des pouvoirs de leur auteur, selon la précision de leur contenu, selon leur objet, selon la plus ou moins grande latitude d'exécution qu'elles laissent à leur destinataire, selon qu'il existe ou non des voies de recours permettant de les contester ou d'en demander la confirmation... Il y a évidemment une grande différence entre une obligation de traitement de données imposée de manière précise par la loi et une obligation légale qui laisse le choix du traitement à mettre en œuvre pour l'exécuter, ou encore entre ces obligations-là et l'injonction d'une autorité émise en vertu de la loi qui pourrait elle aussi porter sur l'obligation d'effectuer un traitement particulier ou simplement sur la communication d'une information en laissant au destinataire le choix des moyens à mettre en œuvre. Une qualification au regard des critères de la LVP ne pourra être établie qu'en tenant compte de toutes les spécificités de chaque situation. Le destinataire d'un ordre peut être responsable de la manière dont il exécute cet ordre tout comme il peut être dépourvu de toute possibilité de choisir.

- **le cas spécifique des transferts de données pour donner suite aux injonctions contraignantes de l'UST**

167. Il n'apparaît pas pertinent de chercher une qualification pour les traitements réalisés par SWIFT aux Etats-Unis sur des données localisées physiquement dans ce pays afin de donner suite aux injonctions contraignantes d'une autorité américaine. En tout état de cause, le droit belge ne s'applique pas sur le territoire des Etats-Unis, et une qualification quelconque resterait purement théorique et sans effet : aucune des obligations de la loi belge ne pourrait être imposée à ce titre.

168. La situation a toutefois pu être source d'ambigüité, SWIFT agissant à deux titres distincts : aux Etats-Unis comme destinataire des injonctions de l'UST et en Europe comme opérateur d'un transfert de données vers un pays tiers. Pour chacun de ces titres, SWIFT était soumis à un droit différent.

169. Il est évident qu'agissant en tant qu'opérateur d'un transfert vers un pays tiers, SWIFT ne pouvait ignorer les changements du niveau de protection dont bénéficiaient les données transférées (contrairement à ce qui aurait pu se passer si les données avaient été transférées à une société tierce). C'est à ce titre, et uniquement à ce titre, qu'aux yeux de la Commission SWIFT devait agir. C'est uniquement à ce titre qu'il faut considérer l'attitude que la société a adoptée, sans égard pour de

supposées obligations qui découleraient de la LVP en conséquence d'une qualification déduite d'une situation soumise au droit américain.

# V. LES MESURES PRISES PAR SWIFT

170. Au cours de l'année qui a précédé le début de la présente procédure, la Commission a entretenu un dialogue suivi avec SWIFT via des courriers détaillés et de multiples réunions[73], dont certaines en présence de représentants du Groupe 29 et du Contrôleur européen de la protection des données (CEPD). La poursuite du dialogue avec SWIFT avait notamment pour but d'encourager cette dernière à développer une nouvelle politique de protection des données à caractère personnel qui, en se conformant aux avis précités, tiendrait mieux compte des réglementations européenne et belge en la matière.

171. De fait, depuis l'adoption de l'avis 37/2006 de la Commission, SWIFT a adopté différentes mesures destinées à mieux garantir la protection des données personnelles traitées à l'occasion des services qu'elle preste. Il s'agit notamment de l'élaboration et de l'adoption de nouvelles polices contractuelles ("policies") relatives à la protection de la vie privée, de l'adhésion aux "principes de la sphère de sécurité" ("Safe Harbor Principles") pour encadrer les traitements réalisés sur le territoire des Etats-Unis, de la décision de modifier l'architecture de son réseau et de la publication et la diffusion d'informations spécifiques aux traitements effectués dans le cadre de ses prestations, tant à destination des institutions financières que du public.

- **De nouvelles polices relatives à la protection des données personnelles**

172. Faisant suite aux griefs formulés, tant par la Commission que par ses homologues européens réunis au sein du Groupe 29, SWIFT a constitué un groupe de travail *ad hoc* ("Data Protection Working Group") composé de responsables des institutions financières considérées par SWIFT comme représentatives de ses membres et utilisateurs. Ce groupe de travail a proposé notamment des modifications à apporter aux diverses polices contractuelles existantes de SWIFT et l'adoption d'une nouvelle police relative à l'adhésion au Safe Harbor (voy. infra).

173. Les travaux du groupe *ad hoc* ont été clôturés en juillet 2007. De nouveaux documents régissant les relations contractuelles de Swift avec ses clients (institutions financières) ont ensuite été adoptés par le Conseil d'administration de Swift et publiés le 20 juillet (notamment sur son site Internet www.swift.com). Les textes adoptés modifient, remplacent ou complètent les anciennes conditions générales et autres documents contractuels de SWIFT. Il s'agit plus particulièrement de :

- La *SWIFT Personal Data Protection Policy*, qui fait la distinction entre les données à caractère personnel collectées pour la gestion de son personnel ou de sa clientèle, et les données à

[73] Les réunions en 2007 avec le secrétariat de la Commission ont eu lieu les 23 mars, 13 avril, 17 avril, 24 mai, 23 juillet et 16 août 2007.

caractère personnel collectées par les clients de SWIFT qui font appel aux services de la société et traitées dans le cadre de ces prestations de services. Dans ce document, SWIFT est qualifiée de sous-traitant au sens de la LVP pour ce qui concerne les traitements de données collectées par les institutions financières et ne s'engage à se conformer qu'aux seules obligations imposées aux sous-traitants par l'article 16 de la LVP[74];

- La *SWIFT Data Retrieval Policy*, qui décrit **(1)** principalement les circonstances et les conditions dans lesquelles SWIFT peut, au bénéfice et à la demande des clients concernés, récupérer et restituer exclusivement à ces demandeurs des données de transfert ou des données contenues dans des messages, lorsque ces données ont fait l'objet d'une sauvegarde temporaire par copie ; la police décrit également les circonstances et conditions dans lesquelles SWIFT serait susceptible d'extraire des données sauvegardées encore en sa possession **(2)** pour les agréger sous forme de résultats statistiques et transmettre ensuite à des tiers ces résultats anonymes (sur demande d'organisations collectives afin d'analyser et de comprendre certains aspects des flux financiers), ou **(3)** éventuellement pour répondre aux réquisitions ou injonctions contraignantes légalement adressées par une autorité compétente en vertu du droit applicable et transmettre ces données à l'autorité concernée ;
- La *SWIFT Safe Harbor Policy* adoptée dans le cadre de l'adhésion de SWIFT aux principes du Safe Harbor (ou principes de la sphère de sécurité), qui s'applique aux transferts européens de données à caractère personnel vers les États-Unis et fournit notamment des informations sur les transferts ultérieurs de données, sur les mesures de sécurité appliquées par SWIFT ainsi que sur la procédure que doivent suivre les personnes concernées pour accéder à leurs données via les institutions financières.

- **L'adhésion aux "principes de la sphère de sécurité" (Safe Harbor)**

174. SWIFT a déclaré, le 19 juillet 2007, son adhésion aux principes de la sphère de sécurité. SWIFT est depuis mentionnée dans le registre public des entreprises adhérentes au Safe Harbor[75] dans le secteur des "services informatiques" ("CSV"). Une police contractuelle relative à la sphère de sécurité a dès lors été adoptée (cf. supra). Ces mesures visaient à rendre le transfert et la conservation aux Etats-Unis de données à caractère personnel dans le cadre des services commerciaux de SWIFT conformes avec les articles 21 et 22 de la LVP.

- **La modification annoncée de l'architecture du réseau de SWIFT**

---

[74] Indépendamment des traitements qui ne concernent pas l'objet de cette recommandation et qui sont décrits par SWIFT dans la catégorie "données à caractère personnel collectées par SWIFT".

[75] Voir http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

175. Le Conseil d'administration de SWIFT a créé un groupe de travail chargé d'examiner différentes options pour la révision de l'architecture du réseau de SWIFT. Suite aux propositions de ce groupe de travail, le Conseil d'administration a décidé[76] en septembre 2007 de modifier l'architecture du réseau et de créer d'ici à la fin 2009 un nouveau centre opérationnel en Suisse[77]. Cette réorganisation de l'architecture consiste à régionaliser les opérations réalisées par SWIFT dans le cadre de ses services, en ce compris le service de "back up" ("Multi-processing zones"). L'objectif est de traiter et d'archiver les messages échangés entre les clients de SWIFT appartenant à la zone économique européenne, y compris la Suisse, uniquement dans des centres opérationnels établis en Europe, à l'exclusion du centre basé aux Etats-Unis.

176. La réorganisation du réseau est motivée par des considérations liées à la protection des données, mais également par des stratégies commerciales[78] visant à prospecter et conquérir de nouveaux marchés régionaux[79], et à améliorer la qualité et les performances des services offerts : la "resilience", la sécurité, la réduction des coûts,...[80]

- **L'information assurée par SWIFT**

177. SWIFT a adopté des mesures visant à assurer une information spécifique aux traitements de données qu'elle réalise.

178. Les clients de SWIFT (les institutions financières) reçoivent une information détaillée[81] sur les traitements mis en œuvre ou susceptibles d'être mis en oeuvre, via les différentes polices, le glossaire en ligne ("Glossary"), les Questions/Réponses mises en ligne et l'assistance personnalisée en cas de besoin. Les nouvelles polices de SWIFT précisent par ailleurs que les institutions

---

[76] voir le communiqué de presse de SWIFT du 4 octobre 2007 sur www.swift.com.

[77] La Commission européenne a reconnu que la Suisse offre un niveau de protection adéquat des données à caractère personnel qui y étaient transférées depuis l'Union européenne. La Suisse est par ailleurs partie à la Convention n°108 du Conseil de l'Europe *pour la protection des personnes à l'égard du traitement automatisé des données à caratère personnel* (cf. infra point 221).

[78] Cf. interview du PDG de SWIFT, M. Lázaro Campos, Dialogue (The Voice of the SWIFT Community), Q2 2007 : "Dans certaines zones qui possèdent un cadre juridique spécifique, notre force commerciale serait renforcée si nos opérations sur les données étaient réalisées dans de nouvelles implantations. SWIFT deviendrait attractif pour un plus grand nombre de secteurs d'activités. A cet égard, la question de la protection des données devrait être un facteur qu'il faudra aussi bien apprécier." ("*In some jurisdictions, our commercial appeal would be improved if we processed data in additional locations. We would attract more business to SWIFT. Data privacy would also be a factor to consider in this context*".)

[79] Les objectifs "SWIFT2010" sont notamment attentifs aux développements programmés du projet SEPA ("Single European Paiment Area")

[80] Réponse de SWIFT du 16 novembre 2007 (point 3.1.iii) aux questions écrites de la Commission.

[81] Sous réserve de certaines informations techniques sécurisées.

financières clientes doivent communiquer à leurs propres clients des informations concernant le traitement de leurs données à caractère personnel effectués à l'occasion des services prestés par SWIFT[82].

179. SWIFT a également rendu accessible au grand public une série d'informations sur les traitements réalisés, via son site internet : publication des polices encadrant les traitements de données ; explications spécifiques concernant les injonctions de l'UST ; réponses aux questions les plus fréquemment posées (notamment : emplacement des centres opérationnels, motif du doublage des traitements et des données, mesures de sécurité mises en œuvre,...).

- **Les déclarations de traitements auprès de la Commission**

180. Dans son avis 37/2006, la Commission estimait que SWIFT avait l'obligation de déclarer l'ensemble des traitements qu'elle réalisait, conformément à l'article 17 de la LVP. Parce qu'elle considérait ne pas être destinataire de l'avis, qu'elle contestait la qualification de responsable de traitement et qu'elle ne se s'estimait dès lors pas tenue par les obligations liées à ce statut, SWIFT n'avait toujours pas introduit auprès de la Commission de déclaration de traitement au moment de l'ouverture de la présente procédure de recommandation.

181. En complément à sa réponse aux conclusions du rapporteur et à l'audience du 8 octobre 2008, SWIFT a déposé auprès de la Commission deux projets de déclarations qui correspondent à l'analyse détaillée des faits et aux distinctions opérées par le rapporteur entre ceux-ci et entre les responsabilités distinctes auxquelles ils conduisent : **(1)** en qualité de délégué de fait de la communauté de ses utilisateurs clients, pour les traitements dont cette communauté est responsable, conformément aux conclusions du rapporteur et à ce qui est exposé supra (points 163 et 164), ainsi que **(2)** en qualité de responsable des traitements à finalité statistique et de recherche.

- **Des mesures destinées à prévenir les problèmes et à garantir l'exercice effectif des droits**

182. En outre, SWIFT a adopté une série de mesures et de procédures internes destinées à vérifier le respect des obligations de la LVP, à prévenir d'éventuels problèmes et à garantir que les personnes concernées par les données à caractère personnel traitées puissent, le cas échéant, exercer effectivement les droits qui leurs sont accordés par la loi.

---

[82] Le Groupe 29 reste à cet égard particulièrement attentif à la qualité de l'information fournie par les banques européennes à leurs clients.

183. Un Privacy Officer a été désigné à temps plein au sein de la société. Il sera à ce titre l'interlocuteur privilégié de la Commission.

184. Une demande légitime formulée par une personne concernée par le traitement de ses données à caractère personnel sera traitée par les services du Privacy Officer. SWIFT n'étant pas en mesure de répondre directement à ces demandes à défaut de moyen lui permettant d'identifier les données pertinentes contenues dans les messages (et ne devant par ailleurs pas supporter la charge principale des obligations liées à ces demandes – cf. infra), il est prévu que la société invite la personne concernée à communiquer le nom de sa banque et transfère à cette dernière la demande en l'invitant à y donner suite et à l'informer du suivi. Cette procédure est déjà expressément visée dans la police relative à la Sphère de sécurité (cf. supra) mais sera appliquée à l'ensemble des demandes légitimes, en particulier celles fondées sur l'application de la LVP.

185. Le "Data Protection Working Group" sera institué de manière permanente et aura pour première tâche de réexaminer les polices de SWIFT pour apprécier la nécessité de les modifier afin de tenir compte des éléments pertinents de la présente décision. Il s'agira notamment de déterminer dans quelle mesure il sera utile de préciser les procédures internes (notamment celle décrite au point précédent) visant à assurer l'encadrement des personnes concernées.

# VI. L'APPLICATION DE LA LOI ET LES OBLIGATIONS DES RESPONSABLES DES TRAITEMENTS

186. Que SWIFT agisse comme délégué de fait de la communauté de ses utilisateurs clients ou qu'elle agisse marginalement en tant que responsable de traitement, il importe de déterminer la portée et le contenu des obligations auxquelles la société serait tenue ou qu'elle devrait supporter.

187. En tout état de cause, il faut préalablement rappeler que, pour les traitements dont elles sont responsables, les institutions financières sont soumises aux obligations du droit qui leur est applicable.

## VI.1. LA COMMUNAUTÉ FINANCIÈRE

188. La communauté financière des utilisateurs clients de SWIFT ne possède pas d'identité précise et stable, ni d'organisation expressément constituée. Or, pour l'application de la LVP et à en suivre les dispositions, le responsable du traitement décide (des finalités et des moyens du traitement), mais il doit aussi pouvoir agir, notamment pour exécuter ses obligations légales. Le responsable du traitement doit agir et s'exprimer de manière identifiable pour les différents titulaires des données traitées, pour les autres responsables de traitement avec lesquels des données sont échangées, et bien entendu pour les autorités de contrôle comme la Commission.

189. Il faut manifestement constater que cette communauté, pour ce qui est des traitements placés sous sa responsabilité (cf. supra n° 163 et 164), agit à travers les structures et les procédures de dialogue qu'elle a choisies en créant la société et ses règles de fonctionnement. SWIFT est bien le catalyseur organisé des volontés des membres de cette communauté, le lieu du dialogue et de la synthèse et, *in fine*, de la concrétisation et de l'expression de la volonté collective (cf. supra). A défaut d'une représentation différente et distincte clairement identifiable, assumée et organisée, et au moins pour ce qui concerne spécifiquement les traitements en cause et l'application de la LVP, SWIFT doit être considérée comme le délégué de fait de la communauté financière de ses utilisateurs clients (cette dernière étant la responsable des traitements concernés), représentant cette communauté dont elle est issue et à laquelle elle est par essence liée, et agissant en son nom[83].

[83] La dénomination retenue ("délégué de fait") correspond le mieux à la situation telle qu'elle a été constatée et décrite. La notion de "représentant de fait" aurait suscité une confusion avec la notion de "représentant" au sens de la LVP. A priori, ce

### VI.1.1. Les obligations qui privilégient ou qui nécessitent un contact avec les personnes concernées : la qualité des données, l'information, les droits d'accès, de rectification et d'opposition

- **De manière générale**

190. SWIFT invoque que si elle devait être considérée responsable de traitement, elle serait tenue de remplir des obligations qui ne lui incombent pas en tant que sous-traitant, que ces obligations nécessiteraient des efforts disproportionnés autant qu'inutiles (par exemple s'il agissait d'opérer des vérifications qui auraient déjà été faites), et que les opérations de grande échelle à accomplir pourraient s'avérer particulièrement dangereuses pour la sécurité des traitements et la confidentialité des données. L'argument doit évidemment être considéré avec autant d'attention pour ce qui concerne les mêmes obligations mises à charge de la communauté financière, s'il fallait considérer que SWIFT, par délégation, était tenue de les exécuter.

191. Effectivement, SWIFT n'exploite pas les données identifiantes des personnes concernées (cf. supra) et ne possède pas d'outil permettant d'accéder aux données traitées via les données identifiantes en sa possession. Aujourd'hui, SWIFT ne pourrait donc exécuter une obligation qui nécessite un contact direct avec les personnes concernées (donner suite aux droits d'accès, de rectification et d'opposition) ou qui suppose au moins un accès aux données identifiantes (vérifier la qualité des données). De même, une information privilégiée directement adressée à chaque personne concernée ne peut pas être effectuée par SWIFT. Si la société était tenue d'agir ainsi, ou si elle décidait de le faire, elle devrait développer un instrument lui permettant de repérer et de gérer ces données identifiantes. Cet instrument, les traitements qu'il impliquerait et les possibilités

---

dernier n'est pas un opérateur intervenant directement dans le traitement des données, et pour les situations qui rendent son intervention nécessaire, semble avoir une personnalité plus nettement distincte de celle du responsable du traitement. La notion de "responsable apparent", sur la base de la théorie de l'apparence, aurait pu sous-entendre une façon d'agir qui excèderait les pouvoirs et les compétences légalement ou contractuellement attribués, et une autonomie décisionnelle de SWIFT, ce qui ne correspond manifestement pas à la manière dont la société est réellement contrôlée et avec laquelle les décisions sont effectivement prises. Au demeurant, l'apparence, dans ce cas-ci, n'engagerait pas la responsabilité de la communauté financière du fait des actes d'un de ses membres, organes ou préposés qui aurait excédé ses pouvoirs ou dont les pouvoirs auraient été publiquement consacrés par un comportement constant et admis. L'apparence aurait pour effet de dissocier SWIFT de la communauté financière, et de consacrer non pas une apparente responsabilité, mais une responsabilité véritable et autonome (le responsable de traitement ne rendant de comptes qu'à lui-même et que pour lui-même) qui ne correspond pas à la réalité. La question n'est pas que théorique. La dénomination choisie, par ce qui la sous-tend et par ce qu'elle consacre, peut avoir des conséquences sur l'application effective de dispositions civiles ou pénales, ce qui ne relève pas des compétences de la Commission. Mais elle peut surtout, si elle n'est pas adéquate, masquer certains aspects spécifiques à l'organisation de la communauté d'intérêt identifiée et empêcher d'en tirer toutes les conclusions utiles (cf. infra, n$^{os}$ suivants).

d'exploitations difficilement contrôlables qu'il ouvrirait, seraient manifestement de nature à nuire à la sécurité des traitements actuellement réalisés et à la confidentialité des données.

192. Il convient malgré tout que les droits des personnes puissent être exercés, ou que le bénéfice que garantissent ces droits leur soit bien acquis.

193. On peut considérer que, par défaut, SWIFT doit supporter et exécuter les obligations auxquelles la communauté financière de ses utilisateurs clients est tenue en tant que responsable de traitement[84], et qu'à cette fin, par défaut toujours, les tiers concernés peuvent s'adresser à elle[85].

194. Il convient toutefois d'apprécier si la délégation de SWIFT et les charges qui en résultent ne sont pas limitées ou circonscrites par d'autres délégations consacrées ou imposées par les faits, par les particularités des liens et des engagements qui unissent les utilisateurs clients de SWIFT ou encore par des impératifs spécifiques à la LVP et à son application.

195. Outre l'existence d'une délégation dans le chef de SWIFT, établie par défaut, pour déterminer concrètement la manière dont les obligations de la LVP sont ou doivent être exécutées dans la circonstance particulière d'un responsable de traitement constitué de fait par la réunion d'une multitude d'entités distinctes, les faits propres à la situation peuvent être appréciés à la lumière des principes suivants :

- les principes généraux régissant les engagements mutuels supposent que chacun des membres d'une communauté (d'autant plus si elle est volontairement constituée afin de poursuivre un intérêt commun) soit naturellement tenu par un devoir de loyauté à l'égard des autres membres de la communauté ;
- plus particulièrement, le principe de l'exécution de bonne foi des engagements mutuels suppose notamment la prise en compte des légitimes expectatives des autres membres de la communauté (et certainement celles dont l'existence est manifeste) et une coopération évidente selon laquelle chacun supporte les obligations qu'il est, incontestablement, le plus apte ou le seul apte à exécuter sans charge excessive ;
- l'application de la LVP, pour ce qui est de la détermination de la responsabilité d'un traitement de données ou de la charge d'une obligation spécifique qui en résulte, n'est pas limitée ou tenue strictement par les dispositions particulières au droit des contrats ou au

[84] Ou à tout le moins en garantir l'exécution.

[85] Dès lors que SWIFT effectue des traitements de données visés par la LVP par délégation de la communauté financière, rien ne permettrait de considérer que cette délégation ne soit pas opposable aux personnes concernées, titulaires des données traitées.

droit commercial ; ainsi, par exemple, la protection des droits et libertés fondamentaux des personnes ne pourrait être contrariée ou neutralisée par la prévalence des règles qui régissent et organisent la responsabilité contractuelle ; la LVP peut ainsi admettre l'imputabilité ("accountability") d'une charge, entre les entités constituant collectivement le responsable du traitement, à celle qui peut la mieux ou la seule supporter ou exécuter l'obligation collective sans effort excessif, en écartant éventuellement certaines règles relevant d'autres domaines du droit à partir du moment où leur stricte application constituerait un obstacle insurmontable à la protection des droits fondamentaux ;

- des engagements unilatéraux, actes d'acceptation ou stipulations volontaires de la part des membres de la communauté sont de nature à renforcer, voire à rendre incontestables, les conclusions et déterminations auxquelles peuvent conduire les principes généraux régissant les engagements mutuels conjugués aux impératifs de la protection des droits fondamentaux des personnes.

196. Concrètement, plusieurs éléments pertinents peuvent être relevés:

- les institutions financières ont (et sont seules à avoir) un contact direct avec leurs clients et exploitent légitimement les données identifiantes de ceux-ci ;
- les traitements placés sous la responsabilité de la communauté financière, à l'intervention de SWIFT, doivent nécessairement et systématiquement être précédés des traitements placés sous la responsabilité de la banque du donneur d'ordre ; ils en dépendent ;
- les données traitées sous la responsabilité de la communauté financière seront nécessairement et dans tous les cas absolument identiques[86] à celles traitées préalablement sous la responsabilité de la banque du donneur d'ordre ;
- en tant que responsable des premiers traitements et à ce titre, mais aussi en vertu des règles et usages de la pratique bancaire, de l'exécution loyale du mandat confié par ses clients, de sa responsabilité à l'égard des partenaires à la transaction, ou encore en vertu de dispositions légales spécifiques[87], la banque du donneur d'ordre a dû opérer les vérifications nécessaires pour assurer la qualité des données traitées et le respect des conditions dans lesquelles elles peuvent être traitées (exactitude, adéquation, pertinence, non excessivité, légalité, absence d'incompatibilité des traitements ultérieurs – tous connus – avec les finalités de la collecte, conservation limitée,...) ;

---

[86] Comme cela a été décrit, la nature et le fonctionnement du système (et une des finalités des traitements réalisés – cf. supra) impliquent et garantissent cette parfaite conformité.

[87] Par exemple en matière de lutte contre le blanchiment ou contre le financement du terrorisme (cf. supra)

- en tant que responsables des premiers traitements, les banques belges et européennes sont obligées d'informer les personnes concernées des destinataires des données collectées et traitées; dans la mesure où les traitements qui seront réalisés par SWIFT (à quelque titre que ce soit) sont connus et acceptés[88] des banques, la loyauté, à laquelle ces dernières sont tenues, les oblige à informer également leurs clients (en qualité de "personnes concernées") de la ou des finalités des traitements que réalisera SWIFT (en qualité de "destinataire" des données) ;
- les traitements placés sous la responsabilité de la communauté financière étant la conséquence nécessaire de ceux placés sous la responsabilité de la banque expéditrice et portant sur les mêmes données, les droits d'accès, de rectification et d'opposition ne pourraient pas être exercé à l'encontre de la communauté financière de manière à produire un résultat différent que s'ils étaient exercés à l'encontre de l'institution financière tenue d'y donner suite en sa qualité de responsable de traitement (et à tout le moins seule capable aujourd'hui d'y donner suite)[89] ;
- de manière générale, en ce qui concerne les obligations de la LVP nécessitant ou privilégiant un contact avec les personnes concernées, les institutions financières sont tenues, à titre personnel et à l'égard de leurs clients, d'effectuer des prestations dont le contenu est identique ou presque aux à celui des prestations à charge de la communauté financière pour les traitements dont cette dernière est responsable ;
- les institutions financières qui utilisent les services de messagerie SWIFT sont nécessairement membres de la communauté des utilisateurs clients de SWIFT ;
- les institutions financières, de manière constante et unanime, ont régulièrement affirmé et confirmé que la société SWIFT était à leurs yeux le sous-traitant de chacune d'entre elles (y compris pour ce qui concerne l'application de la LVP à l'égard de l'ensemble des opérations réalisées par SWIFT) et qu'elles devaient être considérées comme les seules responsables de traitement des données contenues dans les ordres de leurs clients ; cette affirmation (qui n'est qu'un point de vue) n'établit pas par elle-même le statut et la qualification légale de SWIFT ; mais elle permet de considérer que les banques, en s'avançant comme responsables de traitement, étaient disposées à exécuter les obligations légales liées à ce statut (en ce compris pour les traitements que l'examen des faits conduit à placer sous la responsabilité de la communauté financière) et s'engageaient à le faire.

---

[88] A défaut d'être "déterminés" ou "maîtrisés", au sens de la LVP, par les banques, les traitements sont manifestement connus et acceptés d'elles, notamment parce qu'ils font l'objet avec chacune d'un contrat qui les décrit et les encadre.

[89] Les institutions situées sur le territoire de l'Union européenne sont manifestement tenues en vertu des dispositions de la directive 95/46 et des législations nationales qui en assurent la mise en œuvre ; mais les dispositions contractuelles ou nées de l'usage qui encadrent la pratique bancaire et les relations loyales avec la clientèle peuvent plus largement produire le même effet.

197. Les éléments ici exposés, appréciés à la lumière des principes permettant d'établir une éventuelle répartition des charges liées aux obligations d'un responsable de traitement, conduisent très naturellement à imputer à chacune des institutions financières membres de la communauté des utilisateurs clients de SWIFT, la charge d'exécuter les obligations auxquelles la communauté est tenue et dont le contenu est similaire aux obligations devant par ailleurs être exécutées à titre individuel par chacune d'elles pour les traitements placés sous leur responsabilité personnelle. Au reste, ces obligations ne peuvent aujourd'hui être matériellement prises en charge que par les institutions financières, et leur contenu est strictement et exclusivement limité à ce qui concerne leur propre clientèle.

198. La délégation par défaut dont la communauté de ses utilisateurs clients a investi SWIFT et les exigences qui peuvent en être déduites pour ce qui concerne les obligations imposées par la LVP, doivent dès lors être appréciées, circonscrites et limitées par les charges imputables à chaque institution financière membre de la communauté, que toutes acceptent manifestement d'exécuter.

199. Pour ce qui concerne spécifiquement les suites à donner aux injonctions contraignantes d'autorités administratives ou judiciaires, et sans que cela ne présuppose rien quant à la qualification qui devra toujours être appréciée *in casu* (cf. supra), il faut toutefois noter l'existence de ce qui pourrait être considéré comme une délégation expresse de la communauté à SWIFT (dans l'hypothèse où la communauté de ses utilisateurs clients devrait être désignée comme responsable de certains traitements), consacrée par la "Data Retrieval Policy" et dont l'exercice serait dès lors strictement encadré par cette dernière.

- **En ce qui concerne spécifiquement l'obligation d'information**

200. Le responsable dont le ou les traitements sont soumis aux règlementations belges et européennes, est tenu de fournir aux personnes concernées une série d'informations relatives aux traitements dont leurs données personnelles font, feront ou pourraient éventuellement[90] faire l'objet. Ces informations ne doivent pas être fournies à nouveau, même à un autre titre, "si la personne concernée en est déjà informée", que le responsable du traitement ait obtenu les données auprès de cette dernière ou par une autre voie[91]. L'information obligatoirement fournie à titre personnel par les banques est de nature à offrir cette connaissance préalable.

---

[90] Il doit évidemment s'agir d'une éventualité prévisible, sensée se concrétiser lorsque des conditions connues se réalisent.

[91] Art. 9, § 1er, al.1 et § 2, al. 1 de la LVP.

201. La mise à disposition du public par SWIFT d'informations sur les traitements réalisés par la société (cf. supra), participe en outre à l'exécution générale de l'obligation d'information. Cette information publique est de nature à pallier l'éventuelle imperfection de l'information communiquée par les banques, en particulier les banques qui ne seraient pas situées sur le territoire de l'Union européenne.

202. Par ailleurs, tenant compte de ce qui est déjà accompli ou doit être accompli par les banques, il convient de rappeler que le responsable du traitement est dispensé de fournir les informations mentionnées par la loi (ou une partie de ces informations si d'autres ont pu être fournies) "lorsque (...) l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés"[92]. L'impossibilité ou la disproportion des efforts à accomplir doit bien entendu être justifiée et raisonnablement motivée (notamment dans la déclaration de traitement à déposer auprès de la Commission). A cet égard, "peuvent être pris en considération le nombre de personnes concernées ainsi que les mesures compensatrices qui peuvent être [qui ont été] prises"[93]. Les éléments qui précèdent font état de telles mesures.

203. Au demeurant, certaines informations ne devraient pas être fournies (par SWIFT s'il devait être prétendu que la société seule serait en charge de l'information au nom de la communauté financière) "dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données"[94]. Compte tenu de l'information générale qui est assurée et du fait que SWIFT n'exploite pas les données identifiantes contenues dans les messages, et ne possède pas à ce jour d'outil qui permettrait de le faire, ces circonstances seraient manifestement rencontrées pour les traitements en cause.

- **En ce qui concerne spécifiquement les droits d'accès, de rectification et d'opposition**

204. Si, par hypothèse, on devait supposer que les charges particulières de la communauté financière concernant l'accès, la rectification et l'opposition pourraient ne pas être imputables à chacun des membres de la communauté pour ce qui concerne sa propre clientèle, ou si certains voulaient contester cette imputation, on ne pourrait toutefois ignorer les obligations qui existent déjà et par ailleurs dans le chef de chaque institution financière à l'égard de ses clients, en vertu du droit qui lui est applicable et en vertu des règles générales de la pratique bancaire. Une demande d'accès,

---

[92] Art. 9, § 2, al. 2, litt. a et b.

[93] Directive 95/46/CE, Considérant 40.

[94] Art. 9, § 2, al. 1 in fine.

de rectification ou d'opposition directement adressée à SWIFT et qui exigerait que SWIFT y donne elle-même suite, serait manifestement dépourvue d'intérêt[95], clairement disproportionnée[96], et donc abusive.

205. En tout état de cause, il est utile de rappeler que le droit d'opposition ne peut de toute façon être exercé[97] lorsque le traitement "est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie"[98] ou lorsqu'il "est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis"[99].

206. Pour le surplus, SWIFT intervenant pour certifier l'intégrité des données transmises par la banque émettrice et communiquées à la banque destinataire, on peut difficilement imaginer que la société intervienne pour rectifier ces données sans en référer à ces deux intervenants. En imaginant même que SWIFT puisse avoir accès aux données identifiantes des demandeurs, les rectifications que, hypothétiquement, la société opèrerait devraient nécessairement être répercutées vers les institutions partenaires à la transaction (peut-être au mépris de législations contraignantes qui leur imposent de conserver, plus longtemps que ne les conserve SWIFT, des données liées à un ordre de transfert, qu'elles ont les moyens de vérifier et qu'elles auraient toutes les raisons de considérer comme exactes). C'est bien auprès de la banque émettrice que le droit de rectification doit être exercé (tant qu'il peut l'être), celui exercé auprès de SWIFT (théoriquement envisagé) étant sans objet outre l'absence d'intérêt qu'il y aurait à l'exercer. D'ailleurs, des rectifications ne pourraient, hypothétiquement, être apportées par SWIFT qu'à des données de messages temporairement archivés dans les centres de traitement de la société : elles ne concerneraient donc que des transactions financières déjà exécutées. A ce titre, dans la mesure où elles témoignent de ces transactions et des éléments d'information qui ont entouré leur exécution, il faut considérer que les données en cause sont nécessairement exactes.

---

[95] Les informations étant connues ou pouvant être plus facilement obtenues ou rectifiées à d'autres sources.

[96] Évidente disproportion entre l'absence d'intérêt, l'effort à accomplir pour donner suite à une demande pour laquelle SWIFT ne dispose pas aujourd'hui des outils nécessaires et les risques que le résultat de cet effort constituerait (la production de ces outils et les traitements de données supplémentaires réalisés ou rendus possibles).

[97] Art. 12, § 1er, al. 2 de la LVP.

[98] Art. 5, al. 1er, b. : le contrat avec la banque et l'ordre donnée à cette dernière dans le cadre de ce contrat, pour autant bien sûr que chaque partie (et surtout le client de la banque) soit bien informée des conditions et implications du contrat.

[99] Art. 5, al. 1er, c. : l'injonction contraignante (et légale) d'une autorité constitue une telle obligation ; dans la plupart des États aujourd'hui, les banques sont par exemple obligées de dénoncer les ordres suspects sur base de critères qui leur sont communiqués par les autorités (lutte contre le blanchiment, contre le financement du terrorisme...)

### VI.1.2. La publicité (la déclaration du traitement)

207. Agissant par délégation de la communauté de ses utilisateurs clients, SWIFT doit supporter et exécuter l'obligation de déclarer à la Commission, conformément à l'article 17 de la LVP, les traitements que la société réalise et qui sont placés sous la responsabilité de la communauté.

208. Rien n'identifie une délégation dont aurait été spécialement investie une autre personne pour accomplir cette tâche. C'est au nom de la délégation par défaut qui est la sienne que SWIFT doit dès lors intervenir.

209. Les traitements réalisés par délégation et placés sous la responsabilité de la communauté financière pourraient faire l'objet d'une déclaration, regroupés sous la finalité générique : "contribuer à la sûreté des transactions financières par la transmission automatisée et sécurisée d'informations standardisées, intègres et immédiatement exploitables" (éventuellement détaillée et expliquée par la mention de finalités spécifiques distinctes mais liées – cf. supra). Le transfert, les opérations en miroir et l'archivage aux Etats-Unis ne devraient pas faire l'objet d'une déclaration distincte, dans la mesure où ces traitements ne sont pas réalisés à des fins différentes. Le transfert aux Etats-Unis devrait toutefois faire l'objet d'une mention spécifique, conformément à la loi. L'inutilité ou l'impossibilité d'informer directement les personnes concernées devrait également être motivée.

210. Il n'y a aucune objection légale à ce que la déclaration mentionne explicitement la délégation par laquelle SWIFT intervient et identifie la responsabilité effective de la communauté financière des utilisateurs clients de SWIFT (communauté de fait tacitement mais véritablement constituée par une pratique constante et collective en ce qui concerne les services prestés par SWIFT). Une telle mention est d'ailleurs souhaitable pour spécifier la manière dont les droits d'accès, de rectification et d'opposition devraient être exercés. La clarté à l'égard des personnes concernées garantit en outre leur capacité d'agir au mieux de leurs intérêts en cas de dommage civil.

### VI.1.3. L'application de la loi en ce qui concerne les transferts hors de l'Union européenne

211. Les transferts de données personnelles effectués par SWIFT vers un pays non membre de l'Union européenne sont placés sous la responsabilité de la communauté des utilisateurs clients de SWIFT. Ils concernent exclusivement la duplication en temps réel des traitements et l'archivage réalisés aux Etats-Unis à partir des messages initialement accueillis dans le centre de traitement des Pays-Bas.

212. Tant qu'il n'existe pas de règles expresses et pertinentes en la matière entre les membres de la communauté des utilisateurs clients de SWIFT, la charge des obligations liées à cette responsabilité doit être exécutée par SWIFT en tant que délégué de fait par défaut du responsable du traitement.

213. L'article 21 de la LVP impose que "le transfert de données à caractère personnel faisant l'objet d'un traitement après leur transfert vers un pays non membre de [l'Union] européenne, ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat et moyennant le respect des autres dispositions de la présente loi". A défaut de toute autre indication et à défaut qu'il soit établi par une autorité compétente dans une décision opposable que le niveau de protection dans le pays concerné est soit adéquat soit insuffisant, c'est le responsable du traitement (du transfert) qui doit assurer que cette disposition est bien respectée, en prenant en considération tous les éléments de fait et de droit pertinents.

214. Par sa Décision 2000/520/CE du 26 juillet 2000, la Commission européenne a établi que "pour toutes les activités rentrant dans le domaine d'application de la directive 95/46/CE, il est considéré que les "principes de la sphère de sécurité relatifs à la protection de la vie privée" (...) assurent un niveau de adéquat de protection des données à caractère personnel transférées depuis la Communauté vers des organisations établies aux Etats-Unis" pour autant que "l'organisation destinataire des données [se soit] clairement et publiquement engagée à observer les principes mis en œuvre conformément aux FAQ"[100] et respecte les autres dispositions de la Décision et de ses six annexes.

215. L'article 25, § 6 de la directive 95/46/CE impose que "les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission [européenne]."

216. SWIFT, en tant qu'organisation disposant aux Etats-Unis d'un établissement fixe destinataire de données personnelles transférées depuis l'Union européenne, a déclaré son adhésion aux principes de la sphère de sécurité le 19 juillet 2007.

217. De manière générale, il ne peut être contesté que, depuis lors, les transferts de données vers les Etats-Unis sont conformes aux exigences de la LVP et que SWIFT n'a plus à justifier l'adéquate protection dont doivent bénéficier les données transférées et à évaluer la légalité du transfert.

---

[100] Article 1er, §§ 1 et 2 de la Décision 2000/520/CE de la Commission 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 Etats-Unis d'Amérique.

218. Il convient toutefois de rester attentif au fait que la Décision 2000/520/CE ne couvre de manière impérative et incontestable que "les activités rentrant dans le domaine d'application de la directive 95/46/CE". Les matières judiciaires et policières sont clairement exclues du domaine d'application de la directive (dir. 95/46/CE art. 3.2). Par ailleurs, la Cour européenne de Justice a bien précisé que la directive relative à la protection des données (et les habilitations qu'elle instaure) ne s'applique pas au traitement des données collectées d'abord par des acteurs privés et auxquelles on accède ensuite à des fins de sécurité publiques[101].

219. L'annexe IV à la Décision 2000/520/CE, constituant un des documents explicatifs produits par l'administration américaine du Commerce, précise également : "Les principes de la sphère de sécurité contiennent une exception lorsque le droit écrit, les règlementations ou la jurisprudence créent des obligations conflictuelles ou des autorisations explicites (...) Il est clair que lorsque la législation américaine impose une obligation conflictuelle, les organisations faisant ou non partie de la sphère de sécurité doivent se plier à cette législation. (...) Lorsque la loi autorise spécifiquement [une] société à fournir des informations à caractère personnel à des organismes gouvernementaux sans le consentement de la personne, cela constitue une autorisation explicite d'agir d'une manière contredisant les principes de la sphère de sécurité."

220. Il ressort clairement de ce qui précède que les communications de messages (et de données) à l'UST, en exécution des injonctions contraignantes adressées à SWIFT par cette administration, ne sont pas couvertes par l'autorité de la Décision 2000/520/CE de la Commission et ne bénéficient pas à ce titre de la réputation objective et a priori d'adéquate protection.

221. Or, la LVP, contrairement à la directive 95/46/CE, régit aussi les traitements de données personnelles effectués dans un cadre judiciaire ou policier et étend à ces traitements le champ de la protection garantie aux personnes concernées et l'exigence d'une adéquate protection des données transférées et ultérieurement traitées à des fins de sécurité publique. En l'espèce, la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel trouve également à s'appliquer. La Convention n°108 formule également l'exigence d'une adéquate protection des données transférées, y compris lorsqu'elles sont susceptibles d'être traitées à des fins de sécurité publique. Les conditions de la protection exigée par la Convention n°108 sont toutefois beaucoup moins précises et strictes que celles prévues par la

---

[101] CEJ, arrêt "PNR", affaires jointes C-317/04 et C-318/04, 30 mai 2006. Voir également à ce propos P. DE HERT et R. BELLANOVA, La protection des données d'un point de vue transatlantique : l'UE et les USA sur la voie d'un accord international relatif à la protection des données?, étude à la demande de la Commission des libertés civiles, de la justice et des affaires intérieures, publications du Parlement européen (PE 408.320), octobre 2008.

directive 95/46/CE. Mais il demeure donc qu'à défaut d'une décision objective et opposable d'une autorité compétente, le responsable du traitement (le maître du fichier pour la Convention n°108) doit pouvoir apporter les garanties que les données qu'il transfère bénéficieront d'une adéquate protection lors d'un éventuel traitement ultérieur à des fins de sécurité publique par une autorité compétente du pays destinataire.

222. En vertu des articles 24 et 38 du Traité sur l'Union européenne, la Commission européenne et le Conseil de l'Union sont compétents pour conclure des accords internationaux, notamment en matière judiciaire et policière. Pour ce qui concerne les communications de messages et de données à l'UST dans les limites connues des injonctions adressées au titre de la lutte contre le financement du terrorisme, les "Representations" de l'UST accompagnées des réponses de la Commission européenne et du Conseil de l'Union, publiées le 20 juillet 2007 (cf. supra), et l'autorité dont ces documents sont revêtus, ont levé l'éventuelle incertitude quant à l'adéquate protection (au regard des exigences de la loi) des données transférées aux Etats-Unis et ont comblé les limites manifestes de la protection objectivement reconnue qui est garantie par l'adhésion aux principes de la sphère de sécurité. Il est important de souligner que les "Representations" de l'UST visent expressément à établir le respect des règles de protection contenues dans la directive 95/46/CE. Quand bien même celle-ci n'est-elle pas applicable, c'est bien le niveau de protection élevé qu'elle prévoit qui a servi de référence à l'engagement unilatéral de l'UST à l'accord entre les autorités américaines et européennes.

223. On ne peut légalement contester que, par l'autorité des décisions de la Commission européenne, les exigences des dispositions européennes et celles de la LVP sont bien rencontrées ; que, dans la limite de l'ensemble des situations réalisées et prévisibles, connues et décrites, le transfert de données personnelles depuis les Pays-Bas vers le centre de traitement de SWIFT situé aux Etats-Unis est dès lors parfaitement conforme à la loi ; et que par conséquent les traitements ultérieurs au transfert, réalisés spécifiquement à partir des données physiquement archivées dans le centre américain, échappent à l'appréciation de la Commission pour ce qui concerne la qualité du transfert[102], et ce tant que les dispositions des décisions des autorités européennes sont strictement respectées. En tout état de cause, si les règles d'un pays tiers à l'Union européenne peuvent être appréciées pour évaluer la qualité (et donc la légalité) d'un transfert de données (et pour éventuellement l'interdire du fait d'une protection insuffisante), la LVP n'est pas et ne sera

[102] En tout cas dans la cadre d'une procédure qui vise à contrôler le respect de la loi et qui pourrait conduire à adresser des recommandations à un responsable de traitement. L'appréciation de la Commission reste plus libre dans le cadre d'une procédure d'avis, qui pourrait conduire la Commission à se prononcer sur d'éventuelles insuffisances de la loi et sur la nécessité de la modifier.

évidemment jamais applicable sur le territoire de ce pays tiers pour ce qui concerne le traitement des données qui s'y trouvent physiquement localisées.

## VI.2. LA SOCIÉTÉ SWIFT

224. Pour les traitements réalisés occasionnellement, en fonction de circonstances particulières, et dont SWIFT est directement responsable, il convient aussi d'apprécier la portée des obligations légales faites au responsable du traitement et ce que la société pourrait être tenue d'accomplir pour les exécuter.

225. Il convient de souligner que les traitements placés sous la responsabilité de SWIFT sont, seront et ne pourront nécessairement être effectués que sur des données contenues dans une base générale temporaire (l'archivage) dont la constitution et la conservation sont placées sous la responsabilité de la communauté financière.

226. De la manière déjà exposée, les obligations liées à la qualité des données ont déjà été assurées.

227. Le traitement à des fins statistiques ne présente pas d'incompatibilité avec les finalités initiales de la collecte lorsqu'il est effectué dans les conditions fixées par le Roi en vertu de la loi. Ces conditions, dans la mesure où SWIFT procède à l'anonymisation des données exploitées en les isolant des données identifiantes avant leur traitement statistique, sont pleinement rencontrées.

228. De même, l'exercice des droits d'accès, de rectification et d'opposition n'est pas envisageable concernant des données anonymes.

229. Les traitements réalisés marginalement sous la responsabilité directe de SWIFT à des fins statistiques devraient toutefois faire l'objet d'une déclaration de traitement spécifique, ne serait-ce que pour assurer une parfaite transparence à l'égard du processus d'anonymisation et de l'exploitation des informations anonymes.

# VII. CONCLUSIONS

## VII.1. LA NÉCESSITÉ D'APPRÉCIER LES FAITS EN CONTEXTE

- **Pour ce qui concerne les traitements effectués dans le cadre des services fournis par SWIFT**

230. SWIFT s'est considéré comme un sous-traitant pour l'ensemble des traitements de données réalisés par la société dans le cadre de ses prestations commerciales. La société n'a dès lors pas rempli les obligations imposées par la loi aux responsables de traitement, notamment en ne déposant pas de déclaration de traitement à la Commission (et, de fait, en ne déclarant pas le transfert et l'archivage aux Etats-Unis). SWIFT a maintenu cette position après les avis rendus en 2006 par la Commission et le Groupe 29. Ce rappel doit cependant être prolongé d'une mise en contexte. SWIFT dispose d'une unité d'exploitation aux Etats-Unis, vers laquelle sont transférées les données qu'elle traite et où ces données sont archivées temporairement, depuis près de 35 ans, sans que cela soit méconnu. A aucun moment, depuis l'entrée en vigueur de la LVP il y a plus de 15 ans et jusqu'en juin 2006, les activités de SWIFT et les traitements de données réalisés dans ce cadre n'ont fait l'objet de préoccupations, d'interrogations ou d'une attention spécifique par rapport aux règles et obligations des législations successives régissant le traitement de données à caractère personnel. La Commission n'a été saisie ni de plainte, ni d'information justifiant une investigation. De manière générale, aucune autorité ne s'est préoccupée de la situation, n'a suspecté d'éventuelles infractions à la LVP, ni n'a manifesté de crainte quelconque par rapport à un risque possible. L'absence collective d'attention ne constitue pas, bien évidemment, une excuse pour les comportements non conformes à la loi. Mais elle doit fortement nuancer la sévérité des jugements et des appréciations, surtout si aucun élément déterminant ne permet de mettre en cause, dans ce contexte général, la bonne foi de SWIFT et l'absence d'intention doleuse ou frauduleuse. Il faut aussi constater que l'unité d'exploitation de SWIFT a été installée aux Etats-Unis 25 ans avant que n'entrent en vigueur en Belgique les nouvelles dispositions relatives aux transferts de données vers des Etats non membres de l'Union européenne (en 1998). On peut difficilement reprocher à SWIFT de ne pas avoir réorganisé son réseau dès ce moment, alors qu'aucun problème ne semblait se poser.

231. Il convient de souligner encore que dès le premier avis de la Commission en 2006, SWIFT a manifesté sa position par le biais de notes et mémoires argumentés. On ne peut donc lui reprocher une passivité par rapport aux décisions qu'elle contestait. Ces échanges se sont poursuivis jusqu'à la présente procédure, et ont sans doute amené SWIFT, parmi d'autres éléments, à décider des mesures que la société a depuis adoptées, et qui ont été rappelées.

- **Pour ce qui concerne le transfert de données à l'UST**

232. Il ne semble pas contestable que SWIFT était obligée de donner suite aux injonctions de l'UST et ne pouvait matériellement s'y soustraire, notamment parce qu'un de ses deux centres de traitement et d'archivage (et les informations qui y sont physiquement conservées) est situé sur le territoire des Etats-Unis. A tout le moins, il n'est pas critiquable que le conseil d'administration de SWIFT soit arrivé à cette conclusion après avoir manifesté ses objections et obtenu des garanties limitant l'exploitation des données transférées. Il en aurait été manifestement autrement si, se prévalant des effets extraterritoriaux que le législateur américain a entendu donner aux dispositions légales appliquées, l'UST avait enjoint SWIFT de communiquer des données physiquement conservées hors du territoire des Etats-Unis. Il n'est pas pertinent ici de regretter que SWIFT n'ait pas accompli certaines démarches, ni d'avancer qu'elle aurait été obligée de les accomplir en vertu des législations belges et européenne auxquelles elle reste soumise (notamment des démarches informant les autorités belges et européennes de protection des données). Ces considérations seraient aujourd'hui d'autant moins fondées que l'intervention des autorités américaines à l'égard de SWIFT était (même de manière limitée) déjà connue en 2002 et exploitée dans le cadre d'actions internationales de lutte contre le financement du terrorisme. Des démarches d'information vers les autorités européennes de protection des données auraient peut-être été susceptibles d'encadrer différemment les suites données aux injonctions américaines. Toujours est-il qu'en l'attente d'un éventuel encadrement règlementaire établi et partagé par les autorités américaines et européennes, qu'il ne revenait de toute façon pas à SWIFT de négocier, ces démarches, pour importantes qu'elles auraient pu être, n'auraient rien changé à la force obligatoire des injonctions de l'UST. Il faut aussi apprécier que dans la balance des risques que le conseil d'administration de SWIFT a effectué, il a estimé qu'il obtiendrait plus de garanties et de protection pour les données personnelles transmises dans un cadre discuté[103], alors qu'une attitude d'opposition radicale n'en aurait offert aucune, et aurait sans doute conduit les autorités américaines (éventuellement confirmées par une juridiction) à procéder à une saisie de données plus conséquente encore que les lots qui ont été effectivement transférés et dont l'exploitation a pu être contrôlée par des scrutateurs désignés par SWIFT et aujourd'hui par l'émissaire européen de référence. La large diffusion par la presse américaine des faits qui ont attiré l'attention sur SWIFT a certainement libéré la société d'une charge lourde. Mais il n'est possible à personne de supputer sur ce qu'aurait été dans le temps l'attitude de SWIFT sans cette révélation, et de blâmer SWIFT sur cette base.

---

[103] Par la mise en cause discutée de la probable disproportion des premières injonctions et de leur légalité, jusqu'à estimer, du fait des garanties accordées, n'avoir plus d'argument à faire valoir devant une juridiction, permettant d'établir la portée excessive des injonctions suivantes.

233. De manière générale, il semble dès lors difficile de tirer des faits passés les arguments qui justifieraient des poursuites à l'égard de SWIFT, ou une condamnation quelconque.

234. En outre, il faut sommairement rappeler, comme élément d'appréciation supplémentaire, la qualité des traitements réalisés par SWIFT et des procédures et protections qui les encadrent, les sécurisent et préviennent les risques de traitements dommageables ou d'exploitations illégitimes des données, telles que ces procédures et protection ont été ici établies et décrites.

## VII.2. LA NÉCESSITÉ DE TIRER DES ENSEIGNEMENTS UTILES

235. Il faut admettre que le risque d'une exploitation des données transférées par SWIFT aux Etats-Unis n'assurant pas à ces dernières une protection adéquate, n'est pas complètement écarté même s'il demeure théorique.

236. D'autres injonctions administratives contraignantes pourraient être adressées à SWIFT, comme à n'importe quelle organisation établie aux Etats-Unis, poursuivant d'autres objectifs que la lutte contre le financement du terrorisme. Les décisions actuelles ne garantiraient pas, a priori et d'autorité, l'existence d'une adéquate protection des données ainsi obtenues.

237. Qu'il s'agisse de SWIFT[104] ou d'un responsable de traitement placé devant les mêmes contraintes légales (aux Etats-Unis) et les mêmes incertitudes (quant au respect des législations européennes de protection des données personnelles), il serait opportun que les autorités européennes continuent à accorder une attention particulière à cette question, et puissent aboutir à instituer formellement un mécanisme capable d'accueillir le signalement du problème, de garantir la confidentialité de l'information et de supporter officiellement le dialogue et la négociation peut-être nécessaires avec les autorités américaines pour établir des règles de protection adéquate encadrant l'exploitation ultérieure des données requises ou saisies.

238. Aujourd'hui, on ne pourrait raisonnablement imposer aux entités confrontées à des situations similaires, de rapporter seulement et simplement, et sans autre assurance, à l'autorité de contrôle du pays d'origine des données ou même à l'assemblée des autorités européennes de contrôle (G29), des faits à l'égard desquels la loi américaine impose le secret et dont elle sanctionne pénalement la divulgation, et pour lesquels, si un défaut de protection manifeste était constaté, même temporaire, ces autorités ne pourraient légalement garantir la confidentialité. Mais il

[104] Exécutant par délégation les obligations du responsable du traitement.

conviendrait bien évidemment que ces autorités soient associées au mécanisme de régulation et d'encadrement brièvement évoqué.

239. A défaut d'une telle solution, le responsable du traitement que constitue le transfert de données hors du territoire de l'Union européenne restera tenu de garantir l'adéquate protection des données effectivement transférées, et le cas échéant d'obtenir des assurances et des mesures d'encadrement organisant une protection spécifique, quasi sur mesure.

240. L'attitude que SWIFT a adoptée dès 2001 pour faire face aux injonctions qui lui étaient adressées par l'UST a été sévèrement critiquée en 2006, directement après la diffusion des informations publiées par le *New York Times*. La société s'est vu reprocher une attitude légère, voire complaisante, et une violation manifeste des législations belge et européenne de protection des données personnelles. Il convient aujourd'hui d'apprécier ces faits avec une meilleure connaissance, et à la lumière des événements et développements ultérieurs, et d'en tirer, à titre d'exemple, les leçons utiles pour ceux qui demain auraient à assumer les obligations d'un responsable de traitement enjoint sous la contrainte légale de communiquer d'importants fichiers à une administration des Etats-Unis (ou, à contexte équivalent, d'un autre État non membre de l'Union européenne).

241. Il est difficile de déconsidérer les mesures d'encadrement accordées dès 2002 par l'UST à SWIFT en réponse aux objections de la société, si l'on considère que les "Representations" et engagements unilatéraux adressés par la même administration américaine aux autorités de l'Union européenne et acceptés par ces dernières, confirment et maintiennent inchangés toutes les garanties accordées à SWIFT et le fonctionnement du dispositif d'enquête, sous réserve de précisions quant aux délais de conservation des copies de messages obtenues et du rôle attribué à un référent européen indépendant pour contrôler l'ensemble des processus et leur conformité au cadre fixé. Au demeurant, si l'on doit se réjouir de l'existence d'un contrôle mandaté par une autorité publique, les pouvoirs de contrôle, d'audit et d'intervention accordés à l'émissaire des autorités européennes sont les mêmes que ceux dont avaient été investis les scrutateurs indépendants agissant pour le compte de SWIFT.

242. A peu de choses près (et dans la limite de ce que le statut de SWIFT – société privée – lui permettait d'obtenir), les mesures dont les autorités européennes ont estimé qu'elles garantissaient une adéquate protection des données d'abord transférées aux Etats-Unis et ensuite requises par l'UST, sont les mêmes que celles dont SWIFT a bénéficié.

243. Tenant compte des éléments incontestable de légalité internationale invocables[105] et de l'existence d'informations sur les faits portées à la connaissance de certains milieux, mêmes restreints, à l'appui de recommandations officielles aux autres États d'agir de la même manière (cf. supra n° 16), tenant compte aussi de la nature et de l'étendue des garanties accordées à SWIFT dans ce contexte consensuel et de l'acceptation postérieure du caractère adéquat de ces garanties par les autorités européennes, il serait contradictoire et inexact de prétendre aujourd'hui que les communications de données effectuées par SWIFT en exécution des injonctions contraignantes qui lui étaient adressées par l'UST, ne bénéficiaient pas, au regard de notre législation et de ses exigences, d'une protection adéquate avant même les accords entre autorités européennes et américaines.

244. C'est SWIFT qui a assuré l'existence d'un encadrement protecteur effectif. Celui-ci pouvait toujours être plus étendu. Rien par ailleurs n'indique que SWIFT n'aurait pas obtenu plus de garanties encore en adoptant une autre attitude. Mais rien n'indique le contraire non plus. L'attitude de SWIFT n'était peut-être pas la seule adéquate (bien qu'il serait aujourd'hui fort contestable de défendre, hors contexte, d'autres choix supposés meilleurs et évidents), mais on peut dire, quoi qu'il en soit, qu'elle a procédé d'un comportement prudent, diligent et attentif, parmi les enjeux pris en compte, à la protection des données à caractère personnel transférées depuis l'Union européenne. L'on peut d'ailleurs souligner que les garanties accordées aux données européennes ont aussi bénéficié, à la demande de SWIFT, aux données à caractère personnel qui avaient une origine américaine, parce qu'initialement accueillies dans le centre de traitement situé aux États-Unis (cf. supra).

245. Si l'on ne peut en aucun cas en faire un modèle de comportement incontestable à adopter dans des situations similaires, l'attitude de SWIFT peut en tout cas servir de référence. Plus encore, les garanties et protections qui ont été accordées à la société (et l'existence attestée d'une légalité internationale acceptée par la plupart des États) peuvent servir de référence et d'instrument d'évaluation pour prendre attitude et fonder les objections qui pourraient être opposées à des injonctions et des requêtes plus conséquentes, dépourvues du même encadrement et peut-être à ce titre disproportionnées.

246. Le poids de cette responsabilité, laissée au seul responsable des traitements des données personnelles en cause, plaide évidemment pour l'institution et la mise en place rapides des mécanismes européens d'assistance déjà évoqués. L'institution dès novembre 2006 d'un Groupe de

---

[105] S'ils peuvent évidemment être critiqués, faire l'objet de légitimes contestations et fonder des revendications en faveur de décisions en sens contraire, ces éléments de droit existent bien, et ce n'est pas à SWIFT à supporter les critiques qui leur seraient adressées.

contact à haut niveau EU-US sur la protection des données va dans ce sens. L'on pourrait désormais considérer, dans le contexte de relations et échanges nouveaux entre les autorités européennes et américaines, que des situations similaires à celle qu'a connue SWIFT devraient en tout cas, quelques soient les garanties obtenues directement auprès de l'autorité requérante, être portées à la connaissance du Groupe de contact par le responsable de traitement concerné (ou par l'autorité de contrôle spontanément informée). Cette attitude prudente (qui ne dispense pas de mettre en œuvre d'autres moyens tendant à garantir une protection adéquate) ne pourrait faire l'objet de reproches de la part des autorités américaines dès lors que celles-ci se sont précisément engagées à faire examiner les situations problématiques par le Groupe de contact. Cette attitude attesterait d'un exercice loyal et effectif par le responsable de traitement des obligations qui sont les siennes tout en l'assurant d'un appui dans la prise en charge des difficultés auxquelles il pourrait être confronté.

## PAR CES MOTIFS,

- **Quant à la présente procédure de recommandation**

247. Constatant que SWIFT a déclaré auprès de la Commission : **(1)** les traitements qu'elle réalise en tant que délégué de fait par défaut de la communauté de ses utilisateurs clients et **(2)** les traitements soumis aux dispositions de la LVP qu'elle réalise marginalement en tant que responsable, la Commission :

- constate qu'à ce jour SWIFT, agissant par délégation de la communauté de ses utilisateurs clients pour les traitements dont cette dernière est responsable ou agissant marginalement en tant que responsable de traitement, respecte l'ensemble des dispositions de la LVP ;
- décide qu'il n'y a manifestement pas lieu à recommandation ;
- clôt ainsi la présente procédure.

- **Quant aux initiatives prises par SWIFT**

248. Par ailleurs, la Commission prend acte des initiatives propres prises par SWIFT ou par la communauté financière via SWIFT, qui sont de nature ou qui visent directement à renforcer la protection des droits fondamentaux et des libertés des personnes physiques lors des traitements de leurs données à caractère personnel effectués dans le cadre des services prestés par SWIFT, apprécie favorablement ces initiatives et les encourage :

- la décision d'implanter un nouveau centre de traitement en Suisse pour assurer le doublage des traitements et l'archivage temporaire des messages expédiés entre les institutions financières à partir du territoire européen ;
- la désignation d'un Privacy Officer à temps plein au sein de la société;
- la formalisation de procédures encadrant l'exercice de leurs droits par les personnes concernées qui s'adresseraient à SWIFT;
- l'évaluation des polices qui lient SWIFT à ses utilisateurs et clients et qui structurent la communauté d'intérêt que ces derniers constituent.

249. La Commission demande d'être informée des suites qui seront réservées à ces initiatives.

- **Quant aux perspectives pour la communauté financière**

250. La Commission attire l'attention des institutions financières membres de la communauté des utilisateurs clients de SWIFT qui sont situées sur le territoire de l'Union européenne, quant à l'intérêt qu'elles établissent collectivement des règles communes pour assurer l'information à communiquer à leurs clients et garantir l'exercice effectif (lorsqu'il se justifie) des droits d'accès, de rectification et d'opposition concernant les traitements de données réalisés dans le cadre de l'utilisation des services de messagerie SWIFT et placés sous différentes responsabilités successives, étant entendu : **(1)** que chaque institution financière doit naturellement rester chargée de la bonne application de ces règles à l'égard de ses clients ; **(2)** que l'élaboration de ces règles doit faire l'objet d'un accompagnement par le Groupe 29 (sur base des avis que ce dernier a déjà émis) afin d'en garantir la même appréciation dans tous les Etats membres de l'Union européenne.

251. La Commission demande à SWIFT d'informer la communauté financière de ses utilisateurs clients du contenu de la présente décision.

- **Quant aux enseignements utiles qui peuvent être tirés**

252. Conformément à l'article 14 du ROI, la Commission décide de notifier officiellement la présente décision à la Commission européenne et au Groupe 29, en attirant leur attention sur les points 235 à 246, et en souhaitant qu'ils restent saisis de manière effective des questions qui y sont soulevées.

Pour l'Administrateur e.c., Le Président,

(sig.) Patrick Van Wouwe (sig.) Willem Debeuckelaere