Master 2 Professionnel Droit de l'Internet Public
Administration – Entreprises
Présenté et soutenu publiquement
Par Richard MONTBEYRE

Le transfert de données bancaires à caractère personnel vers les Etats-Unis : aspects juridiques de l'Affaire SWIFT

Président du jury : Monsieur Georges CHATILLON, Directeur du Master Droit de l'Internet public
Directeur du mémoire : Monsieur le Professeur Herbert MAISL, Conseiller d'Etat assurant le cours de Droit des données publiques et privées et de leur protection

Avertissement

L'Université Paris I Panthéon – Sorbonne n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire ; ces opinions doivent être considérées comme propres à leur auteur.

Remerciements

Ce mémoire doit beaucoup aux conseils de notre directeur de mémoire, le Professeur **Herbert MAISL**, qui a su nous communiquer son respect pour les libertés fondamentales et dont les cours ont suscité en nous un grand intérêt pour la nécessaire protection des données personnelles.

Les conseils du Professeur **Yves POULLET**, directeur du Centre de Recherche Informatique et Droit de la faculté de droit de Namur, nous ont été d'une aide précieuse, de même que les documents qu'il a nous a fait parvenir.

Nous avons été sensible à la disponibilité de plusieurs autorités nationales et communautaires concernées par notre sujet et regrettons de n'avoir pas eu le loisir de profiter davantage de leur prévenance. Qu'il nous soit permis de remercier à ce titre, le **Parlement européen**, la **Commission européenne**, le **Contrôleur européen de la protection des données**, la **Commission nationale de l'informatique et des libertés** ainsi que la **Commission de la protection de la vie privée**.

Nous savons gré à **Georges CHATILLON**, directeur du Master, qui a su nous a communiquer son énergie et sa passion pour les nouvelles technologies.

Merci enfin à **Aurore RUBIO** pour sa patience dans la relecture et pour la qualité de ses critiques, qui nous ont permis de bénéficier d'un autre regard.

Sommaire

Introduction

Terme employé quotidiennement par les acteurs du monde financier, « SWIFT » ne provoque généralement guère de réactions hors de ce cercle. SWIFT est pourtant à la fois la dénomination sociale d'une société coopérative belge, du réseau mis en place par cette dernière et de la controverse née de l'utilisation secrète de ce réseau par l'administration américaine.

Acronyme de *Society for Worldwide Interbank Financial Telecommunication*, usuellement traduit « Société de télécommunications financières interbancaires mondiales », SWIFT est donc avant tout une société commerciale. Société de droit belge constituée en 1973 par les banques pour gérer les flux de leurs messages financiers, elle délivre ses services à la plupart des institutions financières, qu'il s'agisse de banques, de sociétés de courtage ou de gestionnaires de fonds. Ses 8100 clients, répartis sur plus de 200 pays, donnent la mesure de son importance et de sa position sur le marché de la messagerie interbancaire. Le système mis en place permet de faire circuler des messages normés entre établissements financiers, sans toutefois opérer de transferts de fonds.

Ce système est géré par la société SWIFT SCRL, détenue et contrôlée par ses adhérents. L'entreprise a en effet été constituée sous la forme d'une société coopérative à responsabilité limitée, forme prévue par le droit belge[1]. Les banques clientes de SWIFT sont adhérentes de la société coopérative. Elle est donc étroitement liée au secteur financier qui l'a faite naître.

Quatre années après sa création, la société a été en mesure de créer un réseau rapide et fiable qui a permis de remplacer avantageusement le réseau de communication entre téléscripteurs (réseau « Télex »). Le réseau mis en place a par la suite été remplacé, en 2002-2003, par un réseau reposant sur la technologie *Internet Protocol* (IP). La nouvelle infrastructure de messagerie, baptisée SWIFTNet, permet d'échanger des informations directement avec les entités clientes du service, notamment des entreprises[2].

SWIFT est également la dénomination du réseau qui permet à la société d'offrir un service de messagerie bancaire standardisé sur lequel transitent, par voie électronique, des messages d'information sur les transferts bancaires. Ces messages standardisés sont constitués de codes correspondant aux acteurs de la transaction, mais aussi aux opérations concernées. Ils portent des informations relatives aux transactions et aux virements opérés entre banques. Ils permettent ainsi d'effectuer rapidement des transferts de fonds ou de titres, une fois les négociations conclues. La standardisation des messages permet d'attribuer à chaque banque cliente un code l'identifiant, dit code BIC pour *Bank Identifier Code* ou encore « code SWIFT ». Il convient de donner d'ores et déjà un exemple du fonctionnement du réseau

[1] Pour quelques éléments de définition des SCRL :
Portail fédéral des autorités belges. « Liste des formes de sociétés ». [En ligne]. Consultation le 26/05/07. <http://www.belgium.be/eportal/application?origin=indexDisplay.jsp&event=bea.portal.framework.internal.refresh&pageid=contentPage&docId=6946.0>

[2] Sur les effets de cette migration vers le système IP :
FOUCHARDIERE (de la), Stéphane. « Swifnet révolutionne la manière de concevoir la relation client ». [En ligne]. Site internet du Journal du Net. Publication le 13/06/05. Consultation le 15/06/07.
<http://www.journaldunet.com/solutions/0506/050613_enquete_finance_swiftnet.shtml>

SWIFT, appliqué à une hypothèse simple. La compréhension de l'architecture du réseau est en effet fondamentale pour la compréhension de notre sujet.

Dans l'hypothèse d'un virement bancaire de la France vers les Etats-Unis, une personne A ayant ses comptes en France souhaite verser une somme d'argent à une personne B dont la banque est située aux Etats-Unis. A transmet un ordre de paiement à sa banque. Celle-ci envoie alors, via le réseau SWIFT, un message à la banque de B pour l'informer qu'elle crédite son compte « établissement ». Le message précise également à la banque de B qu'elle doit à son tour créditer le montant au profit de son client B. Nous aurons l'occasion de le rappeler, mais il convient d'ores et déjà de noter que les messages échangés sur le réseau SWIFT comportent la dénomination des parties à la transaction. Or cette dénomination constitue une donnée à caractère personnel au sens de la Directive 95/46/CE[3]. Les messages SWIFT contiennent donc des données protégées par le droit européen (*cf infra*).

Seules des informations ont ici transité sur le réseau, le virement en lui-même – l'opération de transfert de fonds – ne passant pas par l'intermédiaire de SWIFT[4]. Le rôle de SWIFT, s'il est essentiel et constitue le « *centre nerveux du secteur bancaire mondial* »[5], peut donc se résumer à une fonction de messagerie interbancaire. Il n'opère pas de transferts de sommes d'argent. Il n'en demeure pas moins que la société belge est le seul organisme à faire transiter une telle quantité d'informations bancaires puisque la quasi-totalité des transactions financières se traduisent par des messages échangés sur son réseau[6].

Il convient de noter que le système SWIFT repose sur deux pôles : l'ensemble des données échangées sur le réseau sont stockées dans les deux centres opérationnels de la société. L'un est situé aux Pays-Bas, à Zoeterwoude, l'autre aux Etats-Unis, à Culpeper. Chacun des centres contient, à l'heure actuelle, l'ensemble des données échangées. Ce dédoublement des données est à l'origine du transfert de données bancaires à caractère personnel vers les Etats-Unis.

Enfin, SWIFT est une polémique, désignée dans la presse comme l' « Affaire SWIFT », qui repose sur l'utilisation secrète des données de la société par l'administration américaine. Comment une simple société de messagerie bancaire standardisée a-t-elle pu se trouver au cœur d'un véritable scandale impliquant l'administration américaine à son plus haut niveau ? Pour répondre à cette question, il convient de remonter aux événements intervenus le 11 septembre 2001 aux Etats-Unis. Suite à ces événements inédits, l'administration américaine décida de réagir vigoureusement en lançant une véritable « guerre contre le terrorisme ». Le démantèlement des réseaux de financement terroristes est une des armes privilégiées de la lutte, exprimée par le slogan « *Following the money* »[7]. L'*USA*

---

[3] Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible sur le site internet d'accès au droit de l'Union européenne. Article 2.
<http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46>

[4] Les mécanismes de compensation relèvent en effet des chambres de compensation (*Clearstream*, *Euroclear*…) ou des banques elles-mêmes.

[5] LICHTBLAU Eric et RISEN James. « *Bank data is sifted by U.S. in secret to block terror* ». [En ligne]. Site internet du journal *The New York Times*. Publication le 22/06/06. Consultation le 12/03/2007.
<http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200%26en=168d69d26685c26c%26ei=5088%26partner=rssnyt%26emc=rss>
L'article a été publié sur le site internet du journal la veille de la publication sur support papier.

[6] On considère que plus de 10 millions de messages sont échangés quotidiennement sur le réseau SWIFT.

[7] Statement of Under Secretary Stuart Levey on the Terrorist Finance Tracking Program, 23 juin 2003, JS-4334

PATRIOT Act[8], voté par le Congrès et signé par le Président le 26 octobre 2001, sert de cadre juridique à la riposte au terrorisme. Modifié par la suite et complété par de nombreux autres textes d'exception adaptant le droit américain à la lutte contre le terrorisme, il est fortement critiqué du fait des atteintes portées aux libertés individuelles. Il n'en demeure pas moins que ces mesures ont la vertu d'apparaître au grand jour, dans une relative transparence. Elles ne donnent pas toute la mesure de l'action gouvernementale et notre sujet porte ainsi sur une mesure restée inconnue du public pendant cinq ans, jusqu'en juin 2006.

Le 23 juin 2006, le *New York Times (NEW YORK TIMES)* publie en effet un article informant ses lecteurs de l'existence d'un programme secret de pistage des données bancaires destiné à lutter contre le terrorisme, qui attirera quelques jours plus tard les foudres du Président Bush contre le quotidien. Il convient de s'interroger sur les raisons pour lesquelles cet article, intitulé « Les Etats-Unis filtrent les données bancaires en secret pour arrêter le terrorisme »[9], sert de point de départ à ce que l'on désignera désormais « l'Affaire SWIFT ».

L'article, repris le jour même par le *Los Angeles Times* et *The Washington Post*[10], révèle que l'administration américaine consulte sans le contrôle d'aucun juge et dans la plus grande discrétion les données bancaires de la société belge SWIFT. Cette consultation, depuis cinq ans, a lieu par le biais du Département du Trésor et sous couvert de lutte contre les réseaux de financement du terrorisme. Cette révélation provoque des réactions immédiates non seulement aux Etats-Unis mais aussi à l'étranger. Au Etats-Unis, d'abord, parce que ces révélations viennent s'ajouter à celles du même *New York Times*, quelques mois auparavant, sur le programme d'écoute des communications internationales mené par l'Agence de sécurité nationale (NSA)[11]. La révélation de l'Affaire SWIFT sera ensuite reprise par les journaux du monde entier[12].

Avant de développer les implications juridiques de l'Affaire, il s'agit de définir le fonctionnement matériel du programme secret SWIFT. Les modalités matérielles des transferts de données du serveur américain de SWIFT vers le Département du Trésor, concrétisent en effet les accords secrets passés entre la société belge et l'administration américaine. Les données exigées sont physiquement transférées du serveur de la société vers un autre serveur, qualifié de « boîte noire ». Celle-ci est administrée par le Département du Trésor et conservée en ses murs. Ces transferts sont massifs et concernent d'importantes

---

[8] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*. Public Law 107-56, October 21st 2001, (House Resolution 3162).

[9] *Ibid*.

[10] MEYER Josh et MILLER Greg. « *Secret U.S. program tracks global bank transfers* ». [En ligne]. Site internet du journal *The Los Angeles Times*. Publication le 23/06/07. Consultation le 18/03/07. <http://pqasb.pqarchiver.com/latimes/access/1065063511.html?dids=1065063511:1065063511&FMT=ABS&FMTS=ABS:FT&type=current&date=Jun+23%2C+2006&author=Josh+Meyer+and+Greg+Miller&pub=Los+Angeles+Times&edition=&startpage=A.1&desc=U.S.+Secretly+Tracks+Global+Bank+Data>
GELLMAN Barton, BLUSTEIN Paul et LINZER Dafna. « *Bank records secretly tapped* ». [En ligne]. Site internet du journal *The Washington Post*. Publication le 23/06/07. Consultation le 15/03/07. <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300167.html>

[11] En décembre 2005, le *NEW YORK TIMES* a révélé l'existence d'un programme secret de la NSA, consistant à intercepter les communications électroniques de personnes suspectées d'être liées à Al-Qaïda. Or, une loi de 1978, le *Foreign intelligence surveillance Act*, impose à l'administration d'obtenir d'un juge un mandat afin de procéder à de telles écoutes. La révélation de ce programme a suscité de nombreuses réactions d'hostilité contre l'action du gouvernement Bush.

[12] Pour un exemple en France : Le Figaro. « *Comment la CIA épie le financement du terrorisme* ». Paris. [En ligne]. Site internet du journal. Publication le 24/06/07. Consultation le 14/02/07. <http://www.lefigaro.fr/international/20060623.WWW000000341_comment_la_cia_epie_le_financement_du_terrorisme.html>

masses de données. Il convient de noter que l'administration n'y a pas librement accès : pour consulter des données, elle doit interroger la base de données de la boîte noire en précisant sa demande. Cette demande, faite sous le contrôle d'un agent de la société SWIFT, passe par le biais d'un logiciel de recherche en fonction du nom des personnes suspectées par l'administration[13]. Les restrictions posées par SWIFT à la consultation de ses données ne doivent cependant pas faire oublier que ce sont de très grandes quantités de données qui ont été mises à la disposition du Département du Trésor américain.

Il convient de noter que la société SWIFT, exerçant ses activités dans le monde entier, se trouve soumise au droit belge et communautaire de par le lieu de son siège social, mais aussi au droit américain du fait de la localisation de son serveur aux Etats-Unis. Cette double juridiction sur la société explique qu'elle ait pu se trouver, comme ce fut le cas en l'espèce, prise entre deux opinions juridiques contraires. Ainsi, la société a été contrainte, pour obéir au droit américain, de violer le droit européen. A l'opposé, le respect du droit européen des données personnelles aurait conduit SWIFT à violer l'autorité légale attachée aux demandes du Département du Trésor américain. Pour résoudre ce dilemme, la société a fait le choix d'obtempérer aux demandes américaines tout en conservant secrète les violations éventuelles du droit européen, ce jusqu'aux révélations de la presse en juin 2006.

L'Affaire SWIFT soulève un certain nombre de questions fondamentales dans une société mondiale sans cesse à la recherche d'un équilibre entre sécurité et liberté, entre action administrative et droits des citoyens, entre lutte contre des terroristes « ennemis des libertés » et la sauvegarde des libertés fondamentales. En l'espèce, deux positions se sont ainsi affrontées. Nous le verrons, la conception américaine, à l'origine de l'utilisation secrète de SWIFT, justifie cette utilisation par la finalité impérative de lutter sans faillir contre le terrorisme qui a frappé la Nation. De l'autre côté de l'Atlantique, la conception européenne retient une approche toute autre : si les autorités européennes reconnaissent sans difficultés la nécessité de la lutte contre le terrorisme et y contribuent d'autant plus que nombre de pays européens ont subi des attaques violentes, elles attachent une grande importance au respect des libertés fondamentales, quel que soit le contexte actuel.

Alors que l'Affaire intervient dans un contexte marqué par les conséquences des attentats terroristes qui ont frappé indifféremment nombre de démocraties occidentales depuis 2001, la riposte a revêtu des formes distinctes. Sur le plan juridique, alors que les Etats-Unis ont entrepris une profonde réforme de leur droit en général et du droit pénal en particulier, au détriment des libertés individuelles, les Etats européens se sont le plus souvent contentés d'adopter des textes ponctuels, davantage respectueux des libertés. Deux conceptions extrêmement divergentes se sont ainsi développées de part et d'autre de l'Atlantique. Elles se sont affrontées à plusieurs reprises, au fil des affaires mettant en cause à la fois la lutte contre le terrorisme et les libertés fondamentales[14].

Plus spécifiquement, l'Affaire SWIFT touche à une liberté assez récente, qui acquiert une position éminente dans une société reposant de plus en plus sur l'information et le renseignement. Le droit à la vie privée, dans ce contexte, revêt en effet une importance croissante. Le droit à la protection des données personnelles, composante de ce droit à la vie

[13] Commission de la protection de la vie privée. « Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC) ». [En ligne]. Site internet de la Commission. Publication le 27/09/06. Consultation le 25/03/07. p.5-6.
<http://www.privacycommission.be/fr/docs/Commission/2006/avis_37_2006.pdf>

[14] Il n'est que de citer les vols secrets de la CIA en Europe, la guerre en Irak ou encore l'emprisonnement des « combattants étrangers » à la prison de Guantanamo.

privée, fait l'objet d'une protection spécifique, variable selon les différentes régions du monde. A cet égard, nous verrons qu'une fois encore, les variations sont grandes entre l'Union européenne et les Etats-Unis. Considéré comme « fondamental », le droit des données personnelles bénéficie à ce titre d'une protection spéciale en Europe, incarnée par les autorités de protection des données personnelles, qu'elles soient nationales ou communautaires. L'Affaire SWIFT, on le voit, repose autant sur une question de droit que sur une opposition de principe entre deux conceptions politiques.

Du fait de l'importance des enjeux en cause, nous verrons que les autorités politiques ont assez tôt accaparé l'attention jusqu'à éclipser la responsabilité de SWIFT et du secteur financier. Ainsi une simple procédure de réquisition de données, impliquant une filiale américaine de SWIFT et le Département du Trésor, s'est-elle transformée en conflit de souveraineté entre les Etats-Unis et l'Union européenne. Les autorités européennes, qu'elles soient communautaires ou nationales, se sont ainsi en quelque sorte substituées à la société SWIFT pour défendre le droit européen face aux Etats-Unis. Le constat de violation du droit des données à caractère personnel par les autorités chargées de veiller à leur respect a ainsi rapidement été dépassé pour laisser place à des négociations internationales entre l'Union européenne et les Etats-Unis.

La nature politique du conflit a imposé que sa résolution passe, non pas par une action judiciaire dirigée contre SWIFT, mais pas une négociation entre les dirigeants américains et européens. Nous verrons toutefois que l'Affaire, si elle renvoie dos à dos deux entités soucieuses de faire respecter leur souveraineté politique, n'a toutefois pas été résolue sans l'intervention de SWIFT et des autorités de protection des données. Si les négociations internationales ont permis d'apporter des éléments de réponse au conflit politiques, il n'en demeure pas moins que ce sont sans doute les mesures consenties par la société SWIFT qui permettront de protéger au mieux les données personnelles échangées sur son réseau.

On le voit, l'Affaire a oscillé entre la constatation d'une violation du droit à la protection des données personnelles et la résolution politique d'un conflit international. La compréhension de l'Affaire passe donc par la confrontation de deux opinions toutes deux motivées en droit, mais répondant à des préoccupations contradictoires. La mise en place du programme SWIFT par le Département du Trésor répond à la finalité de lutte contre le terrorisme et au droit américain issu des lendemains du 11-Septembre. Elle intervient dans un certain contexte, déterminant pour la création du programme de pistage du financement terroriste dans lequel s'inscrit SWIFT. Nous examinerons à cet égard la légalité du programme au regard du droit américain ainsi que la position de l'administration américaine pour la défense de son programme.

La réaction européenne face à la révélation du programme par la presse, motivée par la volonté de préserver un haut niveau de protection aux libertés fondamentales mais aussi par les inquiétudes provoquée par l'éventuelle utilisation des données de SWIFT à des fins d'espionnage économique ou industriel, devra être précisée. Au-delà de ces inquiétudes quant au fond de l'Affaire, nous verrons que la réaction européenne repose largement sur la dénonciation de l'atteinte à la souveraineté de l'Union européenne et de ses membres, du fait de l'extraction secrète de données considérées comme européennes.

La confrontation des opinions américaine et européenne **(première partie)** nous permettra non seulement de dégager les fondements juridiques et politiques des positions américaine et européenne, qui se sont affrontées à l'occasion de l'Affaire SWIFT, mais également de saisir les prémices de la résolution de cette affaire. Nous verrons en effet que l'Affaire est en bonne voie d'être résolue, grâce à des mesures prises dans deux directions

(seconde partie). Le conflit, cristallisé autour de la contestation du programme SWIFT, a fait l'objet de négociations internationales qui ont récemment permis d'aboutir à l'engagement des Etats-Unis de mieux respecter les principes européens. La résolution de l'affaire a également impliqué le secteur financier, dont la société SWIFT qui a été amenée à revoir ses pratiques en matière de protection des données personnelles et de transparence. La société a en effet consenti à revoir ses pratiques et le monde financier, traditionnellement attaché au secret professionnel et bancaire, a toutefois accepté de voir remis en cause ces caractéristiques parfois synonymes de manque de transparence.

Première partie : Le transfert de données bancaires imposé par l'administration américaine

L'Affaire SWIFT repose sur un programme mis en place par l'administration américaine pour répondre à l'agression terroriste de 2001. Le programme de pistage du financement terroriste, qui procède des pouvoirs d'urgence de l'exécutif américain, est ainsi justifié tant sur le plan juridique que sur le plan politique par la finalité de lutte contre le terrorisme **(A)**. La conformité de ce programme au droit américain ne présumait toutefois pas du respect du droit européen. Nous verrons en effet que ce dernier, qui continue de placer la protection des libertés fondamentales au sommet de sa hiérarchie des normes, retient une approche extrêmement différente qui conduira au constat de la violation du droit fondamental de la protection des données **(B)**.

Chapitre I : La conformité du programme de pistage du financement terroriste au droit américain

Le programme SWIFT, élément fondamental du programme de pistage du financement terroriste, est tout d'abord une arme destinée à défendre les Etats-Unis au lendemain des attentats du 11-Septembre **(1)**. Ce lien de causalité, fondamental pour la compréhension de l'action américaine, ne doit toutefois pas faire oublier que le programme s'inscrit dans un cadre juridique précis et résulte directement des pouvoirs d'exception conférés à l'exécutif suite à la déclaration d'urgence nationale **(2)**.

Section I : Un outil juridique destiné à répondre aux attentats du 11-Septembre

Les attentats du 11 septembre 2001 – La sécurité intérieure comme priorité nationale

Le 11 septembre 2001, des terroristes s'emparent en plein vol de quatre avions commerciaux américains. Deux de ces avions sont délibérément dirigés contre les tours du *World Trade Center* à New York, un troisième sur le Pentagone à Washington et le dernier à Shanksville en Pennsylvanie. Le grand nombre de victimes ainsi que la portée symbolique de l'atteinte portée sur le sol même de la Nation provoque une riposte totale des autorités fédérales. Tous les moyens sont mis en œuvre afin de parvenir à la poursuite et à l'arrestation des auteurs et complices des attentats du 11 septembre, mais aussi en vue de prévenir des attentats ultérieurs. Il est en effet absolument exclu que de telles attaques surviennent de nouveau et la sécurité intérieure devient la première des priorités du gouvernement.

La traque et le démantèlement des réseaux de financement terroristes, moyen de lutte privilégié de l'administration américaine

Parmi les multiples formes d'actions développées pour lutter contre le terrorisme, le « pistage » du financement terroriste a fait l'objet de toute l'attention du gouvernement américain. Au vu des moyens financiers importants déployés par les groupes terroristes pour réaliser leurs attaques, il est rapidement apparu que le démantèlement préventif des réseaux de financement du terrorisme permettrait de prévenir bon nombre d'attentats[15].

Il est en effet avéré que neuf des onze terroristes ayant pris le contrôle des avions le 11 septembre avaient reçu sur des comptes américains des fonds provenant de banques installées en Europe ou au Moyen-Orient[16]. En outre, la fortune personnelle de certaines grandes figures du terrorisme international, le soutien présumé d'Etats qualifiés de « voyous » ou encore les activités illicites sources de revenus importants ont conduit l'administration à s'intéresser de près aux flux financiers impliquant des personnes suspectées. Pour ces raisons, la mise en place d'un programme de pistage du financement terroriste a été l'une des premières mesures prises par le Président des Etats-Unis au lendemain des attentats : dès le 23 septembre, un décret présidentiel confie à l'administration la charge de lutter contre le financement terroriste[17].

Une appréciation finaliste des moyens de lutter contre le terrorisme

Au lendemain des attentats, l'administration américaine et ses théoriciens développent une appréciation finaliste des moyens de lutter contre le terrorisme[18]. Le néo-conservatisme, idéologie adoptée par l'administration mise en place par le Président Bush, intègre sans difficultés la politique de lutte pour la sauvegarde des valeurs américaines à l'intérieur et d'interventionnisme à l'extérieur. Le programme SWIFT, qui contribue à la sécurité des Etats-Unis et permet la traque des terroristes où qu'ils se trouvent, s'intègre donc parfaitement dans un contexte idéologique exacerbé par les attentats[19]. La légitimation finaliste du programme amène à considérer comme accessoires les préoccupations liées aux libertés fondamentales, qui sont simplement rappelées dans leur existence.

Ainsi le Secrétaire du Trésor John W. Snow, la veille de la publication de l'article du *New York Times*[20], insiste sur le fait que « *la sécurité des Américains doit être la première priorité* ». Le communiqué de presse, s'il insiste sur l'efficacité du programme et la fierté de l'administration au vu de ses résultats, est ainsi laconique sur les possibles implications en termes de vie privée. Ce programme, présumé « *conforme aux valeurs démocratiques et aux*

---

[15] Pour une vision globale de la question du financement terroriste : FRANCOIS Ludovic, CHAIGNEAU Pascal et CHESNAY Marc, *Blanchiment et financement du terrorisme*, Paris, Editions Ellipses, 2004.

[16] LICHTBLAU Eric et RISEN James. « *Bank data is sifted by U.S. in secret to block terror* ». [En ligne]. Site internet du journal *The New York Times*. Publication le 22/06/06. Consultation le 12/03/2007. <http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200%26en=168d69d26685c26c%26ei=5088%26partner=rssnyt%26emc=rss>

[17] Il s'agit de l'*Executive Order 13224*, dont nous préciserons la nature et le contenu.

[18] Cette doctrine est notamment incarnée par l'universitaire Paul WOLFOWITZ, devenu Secrétaire-adjoint à la Défense sous la présidence de George W. BUSH. On pourra se référer utilement à : VAISSE Justin et HASSNER Pierre, *Washington et le monde : dilemmes d'une superpuissance*, Paris, Editions Autrement, 2003.

[19] Sur la question de l'encadrement des pouvoirs d'urgence de l'exécutif dans la lutte contre le terrorisme, on pourra utilement consulter l'article de Bruce ACKERMAN, traduit à la revue Esprit.
ACKERMAN Bruce, « Les pouvoirs d'exception à l'âge du terrorisme » in *Esprit*, août/septembre 2006. [En ligne]. Site internet de la revue. Publication en août/septembre 2006. Consultation le 10/06/07. <http://www.esprit.presse.fr/review/article.php?code=13548>

[20] *Cf* note 16.

traditions légales » américaines, est surtout présenté comme un outil permettant de « *rendre l'Amérique et le monde plus sûrs* »[21].

La justification du programme SWIFT réside essentiellement dans les résultats avancés par l'administration. En particulier, elle revendique l'arrestation du plus important représentant du mouvement Jemaah Islamiyah – lié à la mouvance Al-Qaida – en Asie du Sud-est, Riduan Isamuddin dit « Hambali »[22]. Ce dernier est réputé être le chef opérationnel de l'attentat meurtrier du 12 octobre 2002 contre un hôtel à Bali, qui a fait plus de 400 victimes dont 200 morts.

Le Secrétaire du Trésor, John W. Snow, n'a jamais manqué de rappeler que « *l'argent ne ment pas* » et qu'il mène invariablement aux terroristes[23]. Il permet « *de localiser les auteurs d'attentats comme leurs financiers, de retracer les réseaux terroristes, de les amener devant la justice, et de ce fait, de sauver des vies* »[24]. Cette présentation, clairement orientée vers la finalité de l'action anti terroriste, ne se prononce en rien sur l'éventualité d'une atteinte à la vie privée. L'administration suit en effet sa ligne de défense traditionnelle en plaçant la lutte contre le terrorisme au cœur de son argumentation, au prix d'importants sacrifices en termes de libertés individuelles.

Après avoir envisagé le contexte juridique et idéologique du programme SWIFT, il convient de donner quelques précisions sur les réactions qui ont vu le jour aux Etats-Unis à la suite des révélations de la presse en juin 2006. Nous verrons tout d'abord la réaction des autorités gouvernementales face à la révélation d'une de leurs meilleures « armes secrètes » de lutte contre le terrorisme, avant de donner quelques exemples des réactions de l'opinion américaine, cinq ans après les attentats.

La réaction de l'exécutif américain suite à la révélation du programme secret SWIFT

Des représentants du Département du Trésor, informés de la prochaine publication de l'article révélant l'existence du programme SWIFT, ont négocié âprement, mais vainement, avec la rédaction du *New York Times* afin d'éviter que l'information ne soit révélée[25]. La presse, qui semble avoir longtemps hésité sur l'opportunité de cette révélation, a finalement fait le choix de la transparence « *au nom de l'intérêt public* »[26] malgré d'importantes pressions. Ce faisant, elle s'est aliéné l'administration qui révèle, par sa réaction, un sentiment de trahison. Développée le jour même de la publication de l'article du *New York Times* sur

---

[21] Secrétariat du Trésor américain. « *Statement of Treasury Secretary John W. Snow on Disclosure of the Terrorist Finance Tracking Program* ». [En ligne]. Site internet du Département du Trésor. Publication le 22/06/06. Consultation le 15/05/07.
<http://www.treas.gov/press/releases/js4332.htm>

[22] Sous-secrétariat du Trésor américain, en charge de la lutte contre le terrorisme et du renseignement financier. « *Testimony Before the House Financial Services Subcommittee on Oversight and Investigations* ». [En ligne]. Site du Département du Trésor. Publication le 11/07/06. Consultation le 26/04/07.
<http://www.treas.gov/press/releases/hp05.htm>

[23] *Ibid.*

[24] *Ibid.*

[25] The Associated Press. « *U.S. Uses bank records in terror probes* ». [En ligne]. Site internet de la chaîne télévisée. Publication le 23/06/06. Consultation le 27/04/2007.
<http://www.msnbc.msn.com/id/13492032/>

[26] LICHTBLAU Eric et RISEN James. « *Bank data is sifted by U.S. in secret to block terror* ». [En ligne]. Site internet du journal *The New York Times*. Publication le 22/06/06. Consultation le 12/03/2007.
<http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200%26en=168d69d26685c26c%26ei=5088%26partner=rssnyt%26emc=rss>

internet, c'est-à-dire la veille de la publication sur papier, la riposte de l'administration est marquée par une exaspération certaine. Pour s'en convaincre, il n'est que de lire les réactions du Président lui-même.

Alors que son secrétaire du Trésor s'en tient à juger « *regrettable* » la divulgation du programme de surveillance de transactions financières (TFTP), George W. Bush, dès le 26 juin, a non seulement qualifié de « *déplorable* » cette révélation, mais encore déclaré : « *nous sommes en guerre avec des gens qui veulent faire du mal aux Etats-Unis d'Amérique. Que ce soit ceux qui ont permis la fuite d'informations sur ce programme, ou ceux qui les publient, font beaucoup de mal aux Etats-Unis* »[27]. Une semaine plus tard, il renchérissait en n'admettant « *aucune excuse* » à l'attitude de la presse[28]. De son côté, la porte-parole de la Maison Blanche, Dana Perino, n'a pas hésité à se déclarer « *déçue qu'une fois encore le New York Times ait choisi de révéler un programme secret qui protège les Américains* »[29]. Le Sous-secrétaire au Trésor américain en charge de la lutte contre le terrorisme et du renseignement financier, Stuart Levey, est toutefois intervenu dès le 22 juin 2006 dans le cadre d'un entretien télévisé pour expliquer le programme[30].

Au-delà de ces déclarations politiques, le *New York Times* a été menacé de poursuites judiciaires. Le représentant républicain de l'Etat de New York, Peter King, alors Président de la Commission de sécurité intérieure de la Chambre, a qualifié de « *scandaleuse* » l'attitude du journal, qui serait « *davantage concerné par les priorités d'une élite gauchiste que par la sécurité du peuple américain* » et a demandé que la justice se saisisse de l'affaire[31]. Le membre du Congrès considérait qu'il y avait matière à poursuivre le crime de trahison, l'une des plus graves infractions pénales en temps de guerre. La Présidente de la commission judiciaire du Sénat s'est toutefois opposée à cette action en justice qu'elle a jugée « *prématurée* »[32]. Entendu par le Congrès, le Sous-secrétaire au Trésor américain en charge de la lutte contre le terrorisme et du renseignement financier, Stuart Levey, a pour sa part qualifié de « *très dommageable* » la décision de la presse de révéler le programme SWIFT.

Il convient de nuancer ces réactions de l'exécutif en rappelant l'opinion dominante du Congrès. Ce dernier a en effet accueilli ces déclarations avec circonspection, du fait de la mise à l'écart dont il a lui-même fait l'objet : les représentants ont ainsi explicitement regretté d'avoir été laissés dans l'ignorance par le gouvernement quant à l'existence du programme

---

[27] BAKER Peter. « *Surveillance disclosure denounced* ». [En ligne]. Site internet du journal *The Washington Post*. Publication le 27/06/06. Consultation le 03/05/2007.
<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/26/AR2006062600563.html>

[28] SwissInfo. « Espionnage bancaire : Bush toujours très remonté contre la presse ». [En ligne]. Site internet de la Société suisse de radiodiffusion et télévision. Publication le 29/06/06. Consultation le 30/04/2007].
<http://www.swissinfo.org/fre/swissinfo.html?siteSect=105&sid=6855607>

[29] FAURE Guillemette. « La CIA espionne les transactions financières ». [En ligne]. Site internet de la chaîne de radiodiffusion RFI. Publication le 24/06/06. Consultation le 03/05/07.
<http://www.rfi.fr/actufr/articles/078/article_44633.asp>
Le *New York Times* avait révélé l'existence d'un programme de la NSA permettant d'intercepter des communications téléphoniques, quelques mois avant la révélation de l'Affaire SWIFT.

[30] PBS. « *U.S. Government monitors international banking for counterterrorism* ». [En ligne]. Site internet de la chaîne télévisée. Publication le 22/06/06. Consultation le 03/04/07.
<http://www.pbs.org/newshour/bb/terrorism/jan-june06/money_06-23.html>

[31] BURKEMAN Oliver. « *Republican urges prosecution of "treasonous" New York Times* ». [En ligne]. Site internet du journal *The Guardian*. Publication le 26/06/07. Consultation le 02/05/2007.
<http://www.guardian.co.uk/international/story/0,,1805818,00.html>

[32] The Associated Press. « *Lawmaker: Investigate N.Y. Times* ». [En ligne]. Site internet de la chaîne télévisée. Publication le 25/06/06. Consultation le 27/04/2007.
<http://www.msnbc.msn.com/id/13545131/>

SWIFT[33]. Il n'en demeure pas moins qu'un certain nombre de membres républicains du Congrès concernés par les questions de sécurité semble avoir été au courant de l'existence du programme[34] et ont été les premiers à dénoncer la révélation de SWIFT par la presse.

Si la révélation de l'Affaire SWIFT confirme une certaine indépendance rédactionnelle mais aussi le pouvoir de la presse américaine, la forte pression politique, accompagnée de menaces de poursuites judiciaires, a néanmoins contraint le *New York Times* à revoir sa position. C'est ainsi que le médiateur du journal, Byron Calame, a dû publier un revirement d'opinion au titre évocateur : « *Banking data : A mea culpa* »[35]. Il reprend dans cet article l'argumentation de l'administration américaine et admet l'existence du programme ainsi que son caractère secret par la nécessité de sauver des vies. Il explique ce revirement par « *la légalité manifeste du programme* » et « *l'absence de preuve que des données personnelles aient été utilisées de manière illégitime* ». Sa conclusion est claire : le *New York Times* n'aurait pas dû publier l'article. Nous verrons toutefois, du point de vue européen, que c'est cette publication qui a permis à l'Union européenne et aux Etats membres de prendre conscience de l'existence d'un programme violant le droit européen des données personnelles.

La réaction de l'opinion américaine

Le 23 juin 2006, après que la presse ait révélé en détails le programme SWIFT à l'opinion publique américaine, la réaction de l'administration fédérale semble alors ne pas répondre aux attentes : alors que le programme a été délibérément conçu et utilisé en secret, la principale attente consiste en une transparence totale de la part de l'administration. Or cette dernière commence par faire pression sur la presse et par dénoncer une attitude complice du terrorisme. Ainsi les réactions des plus hautes autorités fédérales ne répondent-elles pas à la préoccupation majeure engendrée par le dévoilement de l'Affaire : les libertés fondamentales – dont le droit au respect de la vie privée – sont-elles mises à mal par le programme secret SWIFT ?

Alors que cinq années ont passé depuis les attentats du 11-Septembre, l'opinion publique américaine ne se contente plus de considérations sécuritaires. Le terrorisme, repoussé hors du territoire national, est redevenu une question de politique étrangère. Dès lors, si les Américains acceptent de voir leur pays engagé dans des actions à l'étranger, ils supportent de moins en moins les atteintes à leurs libertés et le silence du gouvernement, malgré les critiques suscitées par son action. Pour légitime que soit l'invocation de la lutte contre les « ennemis de la liberté », il n'est plus accepté que la recherche de la sécurité soit systématiquement opposée à la protection des libertés. Au contraire, l'action antiterroriste doit être conciliée avec le respect des droits fondamentaux et toute action contraire à la sauvegarde

---

[33] The Associated Press. « *Official slams reports of finance monitoring* ». [En ligne]. Site internet de la chaîne télévisée. Publication le 11/07/06. Consultation le 27/04/2007.
<http://www.msnbc.msn.com/id/13814775/>
M. Bu. « Washington, Swift et l'espionnite ». [En ligne]. Site internet du journal La Libre Belgique. Publication le 23/06/06. Consultation le 30/04/2007.
<http://www.lalibre.be/article.phtml?id=10&subid=83&art_id=293530>

[34] The Associated Press. « *U.S. Uses bank records in terror probes* ». [En ligne]. Site internet de la chaîne télévisée. Publication le 23/06/06. Consultation le 27/04/2007.
<http://www.msnbc.msn.com/id/13492032/>

[35] CALAME Byron. « *Banking data: A mea culpa* ». [En ligne]. Site internet du journal *The New York Times*. Publication le 22/10/06. Consultation le 13/04/2007.
<http://www.*New York Times*imes.com/2006/10/22/opinion/22pubed.html?pagewanted=2&_r=2>
Nous traduisons ici par « médiateur » le terme *public editor/ombudsman*. Ce terme correspond en réalité à une personne exerçant à la fois les fonctions d'éditorialiste et de chargé de relations publiques.

des libertés fait l'objet de vives critiques aux Etats-Unis et dans le monde, quand bien même les résultats en termes de sécurité seraient incontestables.

Ainsi, les poursuites contre les individus seulement suspectés de terrorisme, l'incarcération dans des centres de détention spéciaux, les vols secrets de la CIA ou encore la surveillance des communications sont-ils largement dénoncées par les Américains eux-mêmes. Le directeur de l'Association américaine des libertés civiles (ACLU), Anthony Romero, a considéré que le programme SWIFT constitue « *un nouvel exemple des abus de pouvoir de l'administration Bush* »[36]. La réaction d'une partie de l'opinion, qui remet en cause le bien-fondé des moyens employés pour lutter contre le terrorisme, ne présume toutefois pas de la légalité du programme au regard du droit américain en vigueur.

Le cadre juridique d'exception mis en place après les attentats

Si l'agression terroriste subie par les Etats-Unis est sans précédents, la guerre contre le terrorisme dans laquelle le gouvernement américain s'engage se déroule néanmoins dans un certain cadre juridique. Menée par un Etat de droit, l'action anti terroriste doit nécessairement reposer sur des textes juridiques et la riposte, pour exceptionnelle qu'elle soit, passe donc par la mise en place d'une législation propre à encadrer l'action de l'Etat.

Il convient toutefois de noter que l'adaptation du droit à la lutte contre le terrorisme offre de nouveaux moyens au gouvernement sans toutefois accroître le contrôle de légalité sur l'action gouvernementale, le respect des libertés individuelles n'apparaissant pas comme la priorité au lendemain du 11-Septembre.

Le Président Bush, qui souhaite disposer de pouvoirs exceptionnels afin de résoudre la crise déclenchée par les attentats, déclare l'état d'urgence le 14 septembre en vertu du *National Emergencies Act*, trois jours après les attentats[37]. Il offre ainsi à l'administration la possibilité d'agir en vertu de pouvoirs d'urgence. L'état d'urgence a été renouvelé chaque année et demeure donc en vigueur aujourd'hui. Il permet au Président, chef de l'exécutif en vertu de la Constitution[38], de se passer de l'approbation du Congrès pour prendre des décisions qui relèvent en temps normal de la compétence de ce dernier. Chef de l'administration, le Président est également commandant en chef de l'armée et de la marine des Etats-Unis. Il contrôle les départements et agences gouvernementales compétentes en matière militaire. En temps de guerre, il prend les décisions essentielles[39]. Ces pouvoirs militaires sont renforcés par la qualité de chef de la diplomatie accordée au Président.

L'agression de 2001, considérée comme provenant de l'extérieur et ayant provoqué un état de guerre, offre donc naturellement des pouvoirs étendus au Président qui peut empiéter sur ceux du Congrès.

---

[36] *American Civil Liberties Union*. « *ACLU says government spying on bank records is further abuse of power* ». New York. [En ligne]. Site internet de l'association. Publication le 23/06/06. Consultation le 25/06/07. <http://www.aclu.org/safefree/spying/25984prs20060623.html>

[37] Présidence des Etats-Unis. « *Declaration of National Emergency by Reason Of Certain Terrorist Attacks* ». [En ligne]. Site de la Maison Blanche. Publication le 14/11/01. Consultation le 10/07/07. <http://www.whitehouse.gov/news/releases/2001/09/20010914-4.html>
La déclaration d'urgence a été prise en vertu du *National Emergencies Act*, voté par le Congrès en 1976 pour permettre un meilleur contrôle des pouvoirs exceptionnels de l'exécutif.

[38] Article 2 de la Constitution américaine, fixant les pouvoirs de l'exécutif.

[39] Sur les pouvoirs du Président en temps de guerre, on pourra se rapporter utilement à la chronique d'Eileen SERVIDIO-DELABRE. « Chronique de droit américain » [En ligne]. Site collaboratif d'éditeurs CAIRN. Consultation le 26/05/07.
<http://www.cairn.info/search.php?WhatU=%C3%A9tat%20d'urgence&Auteur=&doc=N_RIDP_723_1021.htm&ID_REVUE=RIDP&ID_NUMPUBLIE=RIDP_723&ID_ARTICLE=RIDP_723_1021&DEBUT=#>
Cet article a d'abord été publié à la Revue internationale de droit pénal, Vol.72-2001/3-4, p.1021 à 1034.

Le régime constitutionnel d'exception qui découle de la déclaration d'urgence nationale permet à l'exécutif de disposer des pouvoirs étendus et d'outrepasser ses sphères ordinaires de compétence, sous un contrôle affaibli des contre-pouvoirs que constituent le législatif et le judiciaire. Alors que le Président subit moins sévèrement les contraintes classiques de la séparation des pouvoirs, les agences gouvernementales de sécurité, dépendant directement de la Présidence (FBI, NSA, CIA…), disposent dans ce contexte de moyens juridiques renforcés.

Le pouvoir réglementaire dérivé du Président, très étendu, se double d'un pouvoir réglementaire autonome. Le Président peut, dans le cadre de ce pouvoir réglementaire, prendre des *Executive Orders*[40] que l'on traduit généralement par « décrets présidentiels ». Ces décrets permettent au Président d'intervenir par voie de règlement et constituent donc un outil juridique essentiel de l'exécutif, notamment lorsque ses pouvoirs sont étendus en vertu de l'urgence déclarée. L'*Executive Order* permet ainsi au Président de déléguer certains de ses pouvoirs à son administration, comme ce fut le cas dans l'Affaire SWIFT.

Section II : Un instrument juridique à la disposition de l'administration, découlant des pouvoirs d'urgence de l'exécutif

L'*Executive Order 13224*, fondement juridique de la lutte contre le financement terroriste menée par l'exécutif

Le Président a usé de la possibilité de déléguer ses pouvoirs en confiant au Département du Trésor la responsabilité de lutter contre le financement terroriste, au moyen de *l'Executive Order 13224*[41]. Le Département du Trésor mettra en place le programme SWIFT dans le cadre de ce « décret présidentiel », qui vise deux textes : l'*International Emergency Economic Powers Act* (IEEPA)[42] de 1977 et l'*United Nations Participation Act* (UNPA)[43] de 1945.

L'IEEPA est une loi fédérale votée par le Congrès, qui autorise le Président à déclarer l'existence d'une menace inhabituelle et extraordinaire à la sécurité nationale, à la politique étrangère ou à l'économie des Etats-Unis, provenant de l'extérieur. Elle permet alors au Président, une fois déclaré l'état d'urgence, d'user de pouvoirs étendus en matière économique et financière. Ces pouvoirs incluent la possibilité d'accéder aux transactions financières et aux virements intervenant entre institutions bancaires, dès lors qu'ils impliquent des intérêts étrangers. Le Président peut ainsi bloquer des transactions ou geler des avoirs. En cas d'attaque contre les Etats-Unis, il peut également confisquer les biens des personnes ayant participé ou contribué à l'attaque.

---

[40] La liste des *Executive Orders* pris par le Président depuis 2001 est disponible sur le site de la Maison Blanche : <http://www.whitehouse.gov/news/orders/>

[41] Présidence des Etats-Unis. « *Executive Order on Terrorist Financing – Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit or Support Terrorism* ». [En ligne]. Site internet de la Présidence. Publication le 24/09/01. Consultation le 23/05/07.
<http://www.whitehouse.gov/news/releases/2001/09/20010924-1.html>

[42] *International Emergency Economic Powers Act*. Public Law 95-223, 50 U.S.C. 1701 et seq..

[43] *United Nations Participation Act*. Public Law 79-264, 22 U.S.C. 287c.

L'IEEPA a été largement utilisée par l'exécutif américain, notamment pour limiter les relations commerciales avec certains Etats. A titre d'exemple, on peut citer comme sujets actuels de la loi la Russie, la Biélorussie, l'Iran… Elle peut également cibler des organisations ou des individus précis, ou encore des catégories d'individus[44]. C'est donc naturellement que l'IEEPA a été invoquée par le Président pour confier au Département du Trésor la traque du financement terroriste.

L'*Executive Order 13224*, rendu au visa de l'IEEPA, est également pris au regard de l'art.5 de l'UNPA. Cet acte donne au Président de vastes pouvoirs pour mettre en œuvre les résolutions prises par le Conseil de sécurité des Nations Unies. Parmi ces pouvoirs figure le contrôle des relations financières et des transactions entre des étrangers et les Etats-Unis.

Or, la résolution 1368 du Conseil de sécurité des Nations Unies reconnaît le droit à la légitime défense et condamne les attentats terroristes[45]. Le Président est donc doublement compétent en matière de pistage des réseaux de financements terroristes et peut donc agit en la matière tant en vertu de l'IEEPA que de l'UNPA.

Quant à son contenu, l'*Executive Order 13224* permet au Département du Trésor de prendre toute mesure appropriée pour identifier, enquêter et poursuivre les personnes ayant commis les attentats du 11 septembre ainsi que celles apportant un soutien – quel qu'il soit – à l'activité terroriste. La traque des réseaux financiers terroristes, confiée au Département du Trésor, laisse toutefois une place importante aux agences gouvernementales chargées des questions de sécurité, telles la CIA ou la NSA. Ces dernières pourront bénéficier des renseignements obtenus par le Département, comme ce sera le cas dans l'Affaire SWIFT.

Le *Terrorist Finance Tracking Program* (TFTP), « programme de pistage du financement terroriste » du Département du Trésor

Dans le cadre de la délégation de pouvoirs opérée par l'*Executive Order 13224*, le Département du Trésor a élaboré le *Terrorist Finance Tracking Program* (TFTP), programme destiné à empêcher les attaques terroristes par l'identification et le contrôle des activités financières liées au terrorisme. L'utilisation du système SWIFT pour récupérer des données bancaires sur les transferts d'argent liés au terrorisme constitue une part déterminante de ce programme.

Il convient toutefois de remarquer qu'au moment du lancement du TFTP par le Département du Trésor, nul ne semble avoir songé à se servir de la base de données de SWIFT[46]. C'est un cadre de Wall Street qui en aurait suggéré l'idée à un membre influent de l'administration[47]. L'idée fait rapidement son chemin car l'administration sait que les terroristes du 11-Septembre sont nombreux à avoir reçu de l'argent de l'étranger. L'idée de

---

[44] Il s'agit souvent de terroristes ou de groupes terroristes, mais ce peuvent également être des catégories plus larges : ainsi les personnes impliquées dans des trafics internationaux de stupéfiants depuis 1995 ou encore les personnes contribuant au conflit en Côte d'Ivoire depuis 2006.

[45] Conseil de sécurité des Nations Unies. « Résolution 1368 ». [En ligne]. Site internet des Nations Unies. Publication le 12/09/01. Consultation le 10/07/07.
<http://www.un.org/french/docs/sc/2001/res1368f.pdf>

[46] LICHTBLAU Eric et RISEN James. « *Bank data is sifted by U.S. in secret to block terror* ». [En ligne]. Site internet du journal *The New York Times*. Publication le 22/06/06. Consultation le 12/03/2007.
<http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200%26en=168d69d26685c26c%26ei=5088%26partner=rssnyt%26emc=rss>

[47] *Ibid.*

requérir de SWIFT des informations sur les transferts financiers fut donc retenue par le Département du Trésor. La collecte des données de SWIFT est confiée à l'*Office of Foreign Assets Control* (OFAC), « Bureau du contrôle des avoirs étrangers ». Ce service spécialisé dans la lutte contre le blanchiment d'argent relève du Département du Trésor. Il est directement contrôlé par le Président. C'est par son intermédiaire que des injonctions obligatoires ou « *administrative subpoenas* » seront transmises à SWIFT afin que la société fournisse certaines informations (*cf infra*).

Il convient de noter ici que les données de SWIFT, obtenues secrètement grâce au TFTP, sont ensuite utilisées aux Etats-Unis en vertu du *PATRIOT Act* : une fois leur origine camouflée, ces données permettent ainsi de fonder des poursuites sur le sol américain[48].

L'absence de violation du respect dû à la vie privée en droit américain

Après avoir examiné l'encadrement législatif du programme SWIFT, c'est-à-dire le processus ayant conduit à l'élaboration du *Terrorism Finance Tracking Program* (*cf supra*), il convient d'examiner la conformité du programme à la législation en vigueur et notamment à la Constitution. Nous étudierons ensuite la nature et le contenu de l'instrument juridique utilisé par l'administration pour imposer à SWIFT la communication de ses données, les *administrative subpoenas* (*cf infra*).

La question de la légalité du programme SWIFT se pose d'abord au regard des textes protégeant la vie privée et les données personnelles aux Etats-Unis. Encore faut-il rappeler ici que la Constitution américaine ne garantit pas un droit général au respect de la vie privée, qui protègerait notamment les citoyens contre l'accès par le Gouvernement à leurs informations financières par le biais de tiers[49].

La Cour suprême fédérale a eu l'occasion de se prononcer sur cette question précise dans une affaire bien connue des juristes américains, le cas *United States v. Miller* de 1976[50]. En l'espèce, les chèques bancaires d'une personne poursuivie pénalement avaient été obtenus de sa banque au moyen d'une injonction administrative. Cet individu avait alors invoqué le Quatrième Amendement de la Constitution américaine, qui protège les citoyens contre les perquisitions et saisies abusives. Cet arrêt est considéré comme répondant à la question de savoir si le Quatrième amendement[51] pourrait servir de fondement juridique à un droit général au respect de la vie privée.

La Cour suprême a tranché la question par la négative, donnant une interprétation extrêmement restrictive du champ d'application du Quatrième Amendement : d'une part le

---

[48] ISIKOFF Michael. « *Patriot Act also reveals bank data* ». [En ligne]. Site internet du journal *Newsweek*. Publication le 26/06/06. Consultation le 12/07/07.
<http://www.msnbc.msn.com/id/13561813/site/newsweek/page/0/>
Les données obtenues ont ainsi pu être utilisées devant les juridictions pour fonder des poursuites contre des terroristes. Leur origine comme les modalités de leur obtention étaient alors neutralisées sur les documents présentés aux juges.

[49] Pour une analyse moderne du droit américain des données personnelles :
BIGNAMI Francesca. « *The U.S. Privacy Act in comparative perspective* » in *Colloque sur PNR/SWIFT/Safe Harbour – Les données transatlantiques sont-elles protégées ? tenu à Bruxelles le 26 mars 2007*. [En ligne]. Site internet du Parlement européen. Publication mars 2007. Consultation le 12/06/07.
<http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf>.

[50] Cour suprême des Etats-Unis. *United States v. Miller*, 425 US 435 (1976), décision rendue le 21 avril 1976.
<http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&court=US&vol=425&page=435>

[51] Un exemplaire du *Bill of Rights* publié en ligne sur le site de la *Cornell University Law School* , qui comprend les dix premiers amendements à la Constitution américaine :
<http://www.law.cornell.edu/constitution/constitution.billofrights.html>

texte constitutionnel ne protège que les intrusions dans la vie privée provenant du gouvernement, d'autre part il ne protège que les données de nature personnelle et confidentielle. Il a donc été décidé que « *le Quatrième Amendement n'interdit pas aux autorités gouvernementales d'obtenir des informations [financières] révélées à un tiers* »[52].

Pour tempérer cette interprétation rigoureuse de la Constitution du point de vue des libertés fondamentales, le Congrès a souhaité protéger davantage les informations financières des citoyens. Il a ainsi voté en 1978 le *Right to Financial Privacy Act* (RFPA)[53], loi accordant aux citoyens une protection contre l'accès du gouvernement à leurs documents financiers. Cette loi impose aux autorités de présenter aux institutions financières détentrices des données un acte, qui peut être une *administrative subpoena*. En outre, les autorités doivent notifier à l'individu qu'elles ont accédé à ses données financières.

Ces garanties, qui semblaient imposer à l'administration américaine de prévenir les personnes visées par le programme SWIFT et d'adresser ses demandes aux banques plutôt qu'à la société SWIFT, ont été écartées par le Département du Trésor. Celui-ci, pour justifier le non respect des obligations du RFPA, a rappelé que la loi ne s'applique qu'aux données détenues par des institutions financières : banques, prestataires de services financiers… Or, SWIFT n'est pas considéré comme une telle institution. On considère au contraire que la société ne fournit qu'un service de messagerie standardisé, non constitutif d'une activité bancaire ou financière. Dès lors, l'accès aux données de la société SWIFT n'est pas soumis à cette loi protectrice de la vie privée aux Etats-Unis, la seule qui aurait pu être considérée comme applicable à une telle situation.

Après avoir précisé la légalité du programme SWIFT en matière de protection de la vie privée, au regard de la loi mais aussi de la Constitution, il convient de noter brièvement que la constitutionnalité du programme a pu être remise en cause quant au respect du principe de séparation des pouvoirs. Alors que le Congrès a été largement tenu à l'écart du programme secret SWIFT, la question s'est en effet posée de savoir si l'exécutif n'avait pas violé le système des *checks and balances*, c'est-à-dire de séparation des pouvoirs. En l'espèce, l'exécutif a en effet exigé des données sans passer par l'autorisation de l'autorité judiciaire et sans en référer au pouvoir législatif[54]. Cette question ne semble toutefois pas avoir fait l'objet de controverse de la part du Congrès, passées les premières réactions de surprise, au regard du contexte juridique accordant de larges pouvoirs au pouvoir exécutif (*cf supra*).

Cet arrêt a fait l'objet d'un commentaire éclairant, publié pour la première fois à la revue *Southwestern University Law* en 1978. ALEXANDER Richard et SPURGEON Robert. « *Privacy, banking records and the Supreme Court: a before and after look at Miller* ». [En ligne]. Site internet *The consumer law page*. Consultation le 26/06/07.
<http://consumerlawpage.com/article/privacy.shtml>

[52] *Ibid.*

[53] *Right to Financial Privacy Act of 1978.* [12 U.S.C. 3401 et. seq.]
<http://www4.law.cornell.edu/uscode/html/uscode12/usc_sup_01_12_10_35.html>

[54] Pour quelques éléments de réflexion sur l'Affaire SWIFT au regard des *checks and balances*, voir SCHRADER Jeremy S. « *Secrets Hurt: How SWIFT Shook Up Congress, the European Union, and the U.S. Banking Industry* ». [En ligne]. Site internet de l'institut bancaire de l'université de Caroline du Nord. Publication le 23/02/07. Consultation le 18/06/07.
<http://www.unc.edu/ncbank/Articles%20and%20Notes%20PDFs/Volume%2011/Shrader(397-420).pdf>

La définition des *administrative subpoenas*

Une fois vérifiée la conformité du programme SWIFT au droit au respect de la vie privée tel que défini aux Etats-Unis, il convient de s'intéresser à la pratique par le Département du Trésor des *administrative subpoenas*. Ce terme correspond en effet à une pratique assez inhabituelle de l'administration qui doit être précisée.

Les demandes adressées à SWIFT par le Trésor ont en effet pris la forme d'*administrative subpoenas*, également qualifiées de *compulsory subpoenas*. Ce terme étant délicat à traduire en vocabulaire juridique français, nous conserverons sa dénomination anglaise[55]. La *subpoena*, terme utilisé en droit anglo-saxon, est avant tout un terme latin signifiant littéralement « sous peine de ». En droit positif, il désigne ce que nous qualifierions en droit français de « citation à comparaître devant une juridiction » ou d'« assignation », le refus de comparaître étant passible d'une peine. Le *Dictionnaire juridique de Black* définit plus largement la *subpoena* comme « *un ordre de se présenter à un certain endroit, à un certain moment, pour témoigner* »[56]. La *subpoena* est en principe un ordre donné par une juridiction, qui doit être prise dans le cadre d'une procédure judiciaire.

Au contraire, l'instrument juridique utilisé par le Département du Trésor ne requiert l'intervention d'aucun juge[57]. Les *administrative subpoenas* sont en effet prises par le pouvoir exécutif, le Département du Trésor agissant sur délégation du Président. L'intervention de l'autorité judiciaire n'est pas nécessaire dans ce cas, pour rendre la *subpoena* contraignante. Les *administrative subpoenas* constituent une catégorie d'actes peu ordinaire, contrairement aux *subpoenas* ordinaires. L'empressement de l'administration américaine à présenter la pratique des *administrative subpoenas*, dès le 23 juin 2006, comme la « routine » (en français dans le texte)[58], masque mal le caractère exceptionnel d'une pratique développée peu après les attentats du 11-Septembre. Les *administrative subpoenas* sont, comme leur nom l'indique, obligatoires « sous peine de » sanctions administratives voire pénales, en cas d'inexécution. La personne qui refuserait de s'y soumettre serait ainsi passible de peines d'amende et d'emprisonnement. La dénomination « *compulsory subpoena* » rappelle ce caractère obligatoire, dont il convient de rappeler qu'il ne résulte pas d'une décision judiciaire.

L'*administrative subpoena* est donc un acte officiel émanant de l'administration et ordonnant à un individu de fournir des informations sous peine de sanctions.

La pratique des *subpoenas* par le Département du Trésor dans l'Affaire SWIFT

La compétence de l'administration américaine pour adresser les *subpoenas* à la filiale américaine de SWIFT a été peu discutée, que ce soit par les tenants de l'opinion américaine ou de l'opinion européenne. En effet, SWIFT exerce aux Etats-Unis des activités

[55] Les traductions les plus souvent relevées chez les auteurs francophones pour *administrative subpoenas* sont : « citations administratives », « assignations administratives », « sommations administratives », « injonctions administratives » ou « ordonnances ».

[56] *Black's Law Dictionary*. Saint Paul (Minnesota). West Group. 1999. v° *subpoena*.

[57] LICHTBLAU Eric et RISEN James. « *Bank data is sifted by U.S. in secret to block terror* ». [En ligne]. Site internet du journal *The New York Times*. Publication le 22/06/06. Consultation le 12/03/2007. <http://www.nytimes.com/2006/06/23/washington/23intel.html?ex=1308715200%26en=168d69d26685c26c%26ei=5088%26partner=rssnyt%26emc=rss>

[58] Sous-secrétariat du Trésor américain, en charge de la lutte contre le terrorisme et du renseignement financier. « *Statement of Under Secretary Stuart Levey on the Terrorist Finance Tracking Program* ». [En ligne]. Site internet du Département du Trésor. Publication le 23/06/06. Consultation le 28/04/07. <http://www.ustreas.gov/press/releases/js4334.htm>

substantielles, notamment à Culpeper où est situé un de ses deux centres opérationnels. En outre, s'agissant d'activité commerciale, la compétence fédérale ne fait pas de doute en vertu des textes constitutionnels répartissant la compétence entre Etat fédéral et Etats fédérés.

L'*Office of Foreign Assets Control* (OFAC) a adressé 65 *subpoenas* à SWIFT entre la création du programme et décembre 2006[59]. SWIFT suit un protocole de coopération dit de « *compliance* », qui prévoit la réception de demandes provenant des autorités[60]. La société s'est en effet engagée contractuellement, vis-à-vis de ses clients, à vérifier la légalité des demandes, notamment au regard de la protection des données personnelles. Ainsi, à la réception des *subpoenas*, la société SWIFT a pris soin de consulter de nombreux juristes européens et américaines afin de s'assurer de la validité des demandes administratives. Après que ces juristes aient conclu à la validité des actes, la société s'est exécutée et a livré au Trésor les données requises.

Si la découverte de SWIFT a provoqué quelques remous aux Etats-Unis, il est toutefois important de noter qu'elle n'y a pas été suivie d'une véritable controverse. L'autorité judiciaire comme le pouvoir législatif ne semblent pas avoir considéré l'Affaire SWIFT comme une violation grave du principe des *checks and balances* et il convient de noter qu'aucune action n'a finalement été intentée en justice contre le gouvernement. Il apparaît également qu'une fois passées ses premières réactions, le Congrès n'a pas souhaité mettre en difficulté l'administration et n'a donc pas véritablement contesté l'action du Département du Trésor.

L'absence d'autorité officielle de protection des données personnelles ou de la vie privée a sans doute joué dans ce rapide apaisement de l'Affaire aux Etats-Unis. Sans doute n'y aurait-il même pas eu d'« affaire » sans la polémique suscitée par la réaction européenne à la découverte du programme secret. Il faut toutefois rappeler ici les interrogations et l'inquiétude manifestée aux Etats-Unis par un certain nombre d'associations et de blogs, militant en faveur des droits de l'homme[61]. Si la lutte contre le terrorisme demeure une priorité pour le gouvernement comme pour l'opinion publique, des organisations et des individus ont ainsi pu faire entendre une voix différente de celle de l'administration.

---

[59] Ce chiffre est cité par la Commission à la protection de la vie privée canadienne dans son rapport du 2 avril 2007, disponible en ligne sur le site de la Commission :
<http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_f.asp>

[60] SWIFT S.C.R.L. « *Statement on compliance* ». Bruxelles. [En ligne]. Site internet de la société. Consultation le 12/03/07.
<http://www.swift.com/index.cfm?item_id=6149>

[61] A ce propos, on peut rappeler la réaction de l'*ACLU* (*cf* note 39) et donner l'exemple de l'*Electronic Privacy Information Center* (*EPIC*).
<http://www.epic.org/privacy/surveillance/spotlight/0606/>

Chapitre II : La violation du droit européen des données personnelles

Après avoir vérifié la conformité du programme SWIFT au droit américain, dans un contexte particulier, il convient d'examiner la question de sa légalité au regard du droit européen des données personnelles. Nous envisagerons ainsi la conception européenne des données personnelles, qui explique les vives réactions suscitées en Europe par la révélation du programme secret américain **(1)**. Il s'agira ensuite de préciser les enquêtes diligentées par les autorités européennes, qui constatent une violation grave du droit européen des données mais ouvrent également une voie vers la résolution de l'Affaire **(2)**.

Section I : La conception européenne de la protection des données personnelles

Une compréhension profondément différente des finalités du droit au lendemain du 11-Septembre

Le programme SWIFT est la conséquence des pouvoirs présidentiels exceptionnels accordés à l'exécutif en vertu des textes pris peu de temps après les attentats de 2001. Ce programme est ainsi issu de textes d'exception, spécialement « activés » en 2001 pour renforcer la lutte contre le terrorisme. La perspective du droit européen est toute autre.

En Europe, il est en effet considéré que le programme SWIFT doit avant tout respecter le cadre réglementaire en vigueur, posé par des textes juridiques bien antérieurs aux attentats. Le réflexe européen n'est pas de renouveler en profondeur le cadre juridique au lendemain des attentats mais au contraire de maintenir un haut degré de protection aux individus, en termes de libertés fondamentales. Ainsi l'ordre juridique communautaire et européen, comme celui des Etats membres qu'il contribue à faire évoluer, présentent-ils des caractères très différents de ceux du système américain. Alors que le droit américain pourrait être considéré comme *ad hoc* et dirigé vers un résultat spécifique, le droit européen se veut permanent et garant d'une certaine idée de la société, protégée par le respect des droits fondamentaux des individus. Cette distinction n'est d'ailleurs pas sans rappeler la polémique provoquée par les déclarations sur une « vieille Europe »[62] campée sur ses positions face à un allié américain agacé de ne pouvoir établir de nouvelles règles stratégiques.

Les deux systèmes ne pouvaient donc que s'affronter, tant les préoccupations portées par chacun d'entre eux sont traditionnellement opposées.

Le respect des données à caractère personnel, droit fondamental en Europe

Alors que le système juridique américain ne considère pas le droit à la protection des données personnelles comme un droit fondamental dont la portée serait générale[63] et préfère fractionner la protection au moyen de textes sectoriels, la protection des données personnelles bénéficie au contraire d'une position éminente dans la hiérarchie des normes en Europe. Par l'interprétation que la Cour européenne des droits de l'homme (CEDH) a donnée de l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales

[62] Secrétaire à la Défense Donald H. RUMSFELD. « *Secretary Rumsfeld Briefs at the Foreign Press Center* ». [En ligne]. Site internet du Secrétariat à la Défense. Publication le 22/01/03. Consultation le 24/06/07. <http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=1330>

[63] Affaire *US v. MILLER* (*cf* note 39).

(CESDH)[64], le droit à la protection de la vie privée se prolonge par un droit à la protection des données personnelles depuis l'arrêt Rotaru[65]. La jurisprudence développée par la Cour de Strasbourg en la matière s'est trouvée renforcée par un mouvement analogue suivi par la Cour de justice des Communautés européennes (CJCE). Cette dernière fait en effet application de l'art.6.2 du Traité sur l'Union européenne, qui lui permet de fonder ses décisions sur la CESDH[66]. La CJCE a ainsi annulé les accords conclus entre la Commission européenne et les Etats-Unis à propos des données de passagers du transport aérien (ou « PNR », pour *Passenger name record*)[67].

L'Europe a ainsi fait naître un nouveau droit fondamental à caractère général, conséquence du droit au respect de la vie privée[68].

Il convient de replacer ces considérations juridiques dans ce que Peter Hustinx appelle « *un style européen de la société de l'information* »[69]. Evoquant « *l'interpénétration des vies privées et publiques* », l'actuel contrôleur européen de la protection des données y voit une conséquence de la diffusion toujours plus large des technologies de l'information. Il rappelle que la Charte des droits fondamentaux de l'Union européenne, dont le sort reste suspendu après le rejet du projet de constitution pour l'Europe, comporte un droit spécifique à la protection des données personnelles. Il apparaît que le droit à la protection des données personnelles est l'outil juridique permettant de concilier l'essor des nouvelles technologies et le respect des libertés fondamentales, dans une société qui craint sans toutefois y croire à l'improbable dictature de *Big Brother*.

Les données bancaires de SWIFT, données à caractère personnel protégées par le droit européen

La Directive 95/46/CE, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, définit ces données comme « *toute information*

---

[64] Art.8 : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

[65] CEDH, *Rotaru c. ROUMANIE*, 4 mai 2000, Req. 28341/95. [En ligne].
<http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=700951&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649>

[66] Art.6.2 : « *L'Union respecte les droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres, en tant que principes généraux du droit communautaire* ».

[67] On pourra consulter avec profit la page de l'*Electronic Privacy Information Center (EPIC)* sur cette affaire:
<http://www.epic.org/privacy/intl/passenger_data.html>

[68] Sur la protection européenne des données en Europe : RODOTA Stefano. « *The European constitutional model for data protection* » in *Colloque sur PNR/SWIFT/Safe Harbour – Les données transatlantiques sont-elles protégées ? tenu à Bruxelles le 26 mars 2007.* [En ligne]. Site internet du Parlement européen. Publication mars 2007. Consultation le 27/06/07.
<http://www.europarl.europa.eu/hearings/20070326/libe/rodota_en.pdf>

[69] HUSTINX Peter. « Vie privée et données personnelles : vers un 'style européen de la société de l'information' » in *Les dossiers européens*, février 2007.

concernant une personne physique identifiée ou identifiable »[70]. Le texte précise qu'est réputée identifiable « *ne personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ». Or les messages échangés sur le réseau SWIFT comportent tous la mention des personnes physiques ou morales impliquées dans la transaction. Les clients des banques sont en effet nommément désignés. Ce sont d'ailleurs ces noms qui permettent au Département du Trésor d'interroger la base de données de la « boîte noire » constituée à partir des données exigées de SWIFT par *subpoenas*. Le transfert de données de SWIFT vers l'administration américaine porte donc bien sur des données à caractère personnel au sens du droit européen.

Premières réactions des autorités européennes face à la révélation du programme SWIFT

A la révélation de l'Affaire, les autorités européennes ont immédiatement réagi, avec une certaine virulence. La surprise est en effet la première réaction de ces autorités, qui ne disposent alors sur le programme secret SWIFT que des informations avancées par la presse. Il faudra donc attendre que soient entamées les premières enquêtes pour disposer d'éléments plus solides.

Le Gouvernement belge a émis la volonté d'éclaircir l'affaire par la voix de sa ministre de la Justice, en ouvrant dès le 24 juin 2006 deux enquêtes sur l'utilisation de SWIFT par l'administration américaine[71]. Une de ces enquêtes a été confiée directement à la Sûreté de l'Etat, l'autre à une autorité administrative indépendante de lutte contre le blanchiment d'argent d'origine criminelle[72].

La Commission de la protection de la vie privée belge (CPVP)[73] a pour sa part réagi en ouvrant d'office une enquête dès le 5 juillet 2006, en vertu de l'article 32 de la loi relative à la vie privée qui lui permet de s'autosaisir des dossiers concernant des traitements « *très sensibles* »[74].

---

[70] Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible sur le site internet d'accès au droit de l'Union européenne. Article 2.
<http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46>

[71] Le Soir. « Enquête sur l'espionnage américain ». [En ligne]. Site internet du journal. Publication le 24/06/06. Consultation le 30/04/2007.
<http://www.lesoir.be/actualite/belgique/2006/06/24/article_enquete_ouverte_sur_swift.shtml>
A noter que, selon d'autres journaux belges cités dans l'article, l'affaire était connue de la ministre de la Justice ainsi que du ministre des Finances dès avril 2006 grâce aux informations transmises par la Banque nationale de Belgique (BNB).

[72] Cette autorité est la Cellule de traitement des informations financières (CTIF).

[73] La Commission de la protection de la vie privée est un organisme indépendant créé par la loi du 8 décembre 1992, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Elle veille à ce que les données à caractère personnel soient traitées dans le respect de ladite loi, de manière à préserver la vie privée des citoyens. Elle est le pendant belge de la Commission nationale de l'informatique et des libertés française.
<http://www.privacycommission.be/fr>

[74] Commission de la protection de la vie privée. « Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC) ». [En ligne]. Site internet de la Commission. Publication le 27/09/06. Consultation le 25/03/07.
<http://www.privacycommission.be/fr/docs/Commission/2006/avis_37_2006.pdf>

Le Parlement européen a voté le 6 juillet 2006 une résolution qui marque sa préoccupation générale quant à la dégradation des libertés dans le contexte de lutte contre le terrorisme[75]. Cette résolution prévoit que soit adressée une demande d'éclaircissements à la Commission européenne, au Conseil européen et à la Banque centrale européenne sur leur connaissance de l'accord secret entre SWIFT et le gouvernement américain[76]. Elle prévoit également l'organisation d'auditions publiques par sa commission des libertés civiles, de la justice et des affaires intérieures ainsi que sa commission des affaires économiques et monétaires[77]. Le Parlement, qui a découvert le programme secret SWIFT par la presse, démontre ainsi son attachement aux libertés tout en demeurant prudent sur l'éventuel constat de violation des règles européennes dans cette affaire. Le Parlement a très tôt pris des mesures afin de vérifier la crédibilité des informations révélées par la presse américaine et de pouvoir se prononcer plus surement. La résolution exprime toutefois d'ores et déjà une dénonciation du caractère secret de certaines activités menées par l'administration américaine jusque sur le territoire de l'Union européenne[78].

De son côté, la CNIL a publié un communiqué de presse le 12 juillet 2006 pour rapporter les inquiétudes exprimées par le Parlement européen dans la résolution précitée. Ce communiqué évoque également les contacts pris par la CNIL ainsi que les mesures d'enquêtes envisagées[79]. La Commission n'exprime en revanche aucune réprobation quant au programme SWIFT.

Le Groupe de l'article 29[80] a pour sa part réagi par le biais d'un communiqué de presse le 28 juillet 2006, pour annoncer la coordination des autorités européennes chargées de la protection des données « *afin d'aboutir à une parfaite compréhension de la situation* »[81].

De ces réactions éparses, il convient de relever quelques traits communs. Si peu d'autorités ont dénoncé dans l'immédiat les moyens employés par l'administration américaine, la plupart d'entre elles se sont attachées à vérifier rapidement les allégations de la presse américaine et à demander des auditions et des enquêtes sur le programme américain de pistage du financement terroriste. Une fois passée la réaction de surprise et de suspicion, les principales enquêtes réalisées en Europe à propos de l'Affaire SWIFT ont été menées par la

---

Le paragraphe 1 de l'article 32 de la LVP permet à la Commission de se saisir d'office d'un dossier concernant les traitements « *très sensibles* ».

[75] Parlement européen. « Résolution du Parlement européen sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains ». [En ligne]. Site internet du Parlement. Publication le 06/07/06. Consultation le 04/03/07.
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0317+0+DOC+XML+V0//FR>

[76] Paragraphe 5 de la résolution.

[77] Paragraphe 14 de la résolution. Ces deux commissions permanentes du Parlement européen correspondent aux deux matières concernées par l'Affaire SWIFT. La commission des libertés civiles est présidée par Jean-Marie CAVADA, la commission des affaires économiques par Pervenche BERES.

[78] Paragraphe 13 de la résolution.

[79] CNIL. « Affaire SWIFT : Que fait la CNIL ? ». [En ligne]. Site internet de la Commission. Publication le 12/07/06. Consultation le 02/03/07.
<http://www.cnil.fr/index.php?id=2048>

[80] Le Groupe de l'article 29, a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. Il relève de la Commission européenne.
<http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm>

[81] Groupe de l'article 29. « Communiqué du groupe de travail article 29 sur l'affaire Swift ». [En ligne]. Site internet de la Commission européenne. Publication le 28/07/06. Consultation le 11/04/07.
<http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_28_07_06_fr.pdf>

Commission de la protection de la vie privée belge (CPVP), le Parlement européen, le Groupe de l'article 29 (G29) et le Contrôleur européen de la protection des données (CEPD).

Nous insisterons tout d'abord sur l'avis de la CPVP[82], concernée à plusieurs titres : la société SWIFT est établie en Belgique, à la Hulpe, et La Banque nationale de Belgique exerce une influence prépondérante au sein de son conseil de surveillance. L'autorité de protection des données personnelles belge était donc désignée, parmi les autorités nationale des Etats membres, pour mener l'enquête la plus diligente et la plus approfondie. Nous comparerons son avis avec l'opinion des trois institutions communautaires s'étant saisies de l'Affaire : le Parlement européen, la Commission par la voix du G29 et le CEPD. Ainsi que nous aurons l'occasion de le rappeler, l'Affaire SWIFT présente en effet une forte dimension internationale. Le réseau SWIFT traite en effet les messages concernant la plupart des transactions réalisées entre institutions financières, dispose d'un centre opérationnel de traitement aux Etats-Unis, et se trouve soumis à des systèmes juridiques extrêmement différents. Assujettie au droit européen et au droit américain, la société SWIFT se trouve pour ces raisons au milieu d'un conflit de normes juridiques.

Section II : Les enquêtes européennes sur la révélation du programme SWIFT

L'avis rendu par la Commission de la protection de la vie privée le 27 septembre 2006

L'examen le plus approfondi de l'affaire réalisé par une autorité nationale de protection des données personnelles réside dans l'analyse opérée par la CPVP à la demande des services de renseignement belges. S'il peut paraître surprenant qu'un organe de renseignement passe par la CPVP, il est possible de trouver un commencement d'explication dans les remarques d'un observateur quant à l'efficacité toute relative de ces services[83].

L'avis n°37, rendu le 27 septembre 2006, présente ainsi les fondements juridiques susceptibles d'entraîner des poursuites à l'encontre de la société SWIFT pour violation des textes nationaux et européens protecteurs des données personnelles. Ces textes sont la loi du 8 décembre 1992 (LVP)[84] ainsi que la Directive 95/46/CE du 24 octobre 1995[85]. Il convient d'ajouter à ces textes l'article 8 CESDH, qui garantit le droit à la vie privée et duquel a été tiré le droit à la protection des données personnelles. Dans la mesure du possible, nous nous

---

[82] Commission de la protection de la vie privée. « Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC) ». [En ligne]. Site internet de la Commission. Publication le 27/09/06. Consultation le 25/03/07.
<http://www.privacycommission.be/fr/docs/Commission/2006/avis_37_2006.pdf>

[83] Ph. G. et M. Bu. « Swift : L'injonction était légale ». [En ligne]. Site internet du journal La Libre Belgique. Publication le 27/06/06. Consultation le 30/04/07.
<http://www.lalibre.be/article_print.phtml?art_id=293892>
Cet observateur remettait en cause la capacité des services de renseignement belges à « *aller vérifier ce que la CIA a demandé à telle ou telle firme depuis les Etats-Unis* » avec une certaine ironie.

[84] Loi du 8 décembre 1992, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Disponible sur le site internet de la CPVP.
<http://privacy.fgov.be/fr/static/pdf/wetgeving/loi_vie_privee.pdf>

[85] Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Disponible sur le site internet d'accès au droit de l'Union européenne.
<http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46>

réfèrerons essentiellement aux articles de la Directive plutôt qu'à la LVP belge. La raison de ce choix est simple : la Directive ayant été transposée dans tous les Etats membres de l'Union, on peut supposer que l'argumentaire basé sur des violations constatées au visa de la Directive serait valable pour tout Etat membre[86]. Nous nous efforcerons de saisir les questions de droit susceptibles de se poser dans chaque Etat membre.

Il convient d'apporter ici une précision importante : les directives n'étant pas d'effet immédiat, elles n'obligent les Etats membres qu'en leur imposant de transposer les règles prévues au niveau communautaire dans un certain délai. Elles ne sont pas d'effet direct et ne s'imposent donc pas directement aux sujets de droit national, qu'ils soient des personnes physiques ou morales. Ces personnes ne peuvent en principe se voir reprocher de violer la Directive 95/46/CE et ne peuvent être poursuivies que pour des violations aux règles transposées en droit interne. SWIFT ne peut donc violer que les lois nationales de protection des données. Nous ne nous réfèrerons donc à la Directive que pour mieux constater une violation du droit européen, sans nous limiter au cadre belge.

L'applicabilité des prescriptions de la Directive aux traitements opérés par la société SWIFT

Pour être pleinement assujettie aux obligations posées par la Directive, la société SWIFT doit être reconnue comme responsable du traitement des données qu'elle fait circuler sur son réseau. Or est responsable du traitement, au sens de la Directive, « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* »[87].

SWIFT conteste cette qualification, afin d'échapper aux obligations afférentes en vertu de la Directive. La société indique que la nature même de sa fonction de messagerie des institutions bancaires fait obstacle à la reconnaissance de la qualité de responsable de traitement. Elle se considère comme un prestataire comparable à un « *service postal de télécommunications* », simple sous-traitant des banques et autres institutions financières lui confiant la transmission de leurs messages. Cette qualification de sous-traitant permettrait à SWIFT d'être soumis à des obligations moins rigoureuses et donc de voir sa responsabilité réduite.

La CPVP insiste assez longuement sur la qualification de SWIFT comme responsable du traitement[88]. Elle rappelle tout d'abord le critère de détermination d'un tel responsable : est responsable la personne ayant une « emprise » sur le traitement de données, en application de la définition donnée par la Directive 95/46/CE. Il s'agit donc d'un critère fonctionnel.

Pour retenir la qualité de responsable du traitement SWIFTNet Fin à la société SWIFT, la CPVP relève que le système SWIFT repose sur un réseau international à forte gestion centrale. Or cette gestion est confiée à la société SWIFT SCRL qui joue un rôle bien plus important qu'un simple prestataire de service. En outre, la société détermine la finalité et les moyens du traitement des données[89]. Pour écarter la qualification de sous-traitant, la

[86] Cette assertion se trouve vérifiée par la lecture de l'avis du G29, qui reprend largement l'argumentation de la CPVP et parvient aux mêmes conclusions (*cf infra*).
[87] Article 2 de la Directive.
[88] *Ibid.*, p. 9 à 13 de l'avis.
[89] La société détermine les standards techniques de ses messages et peut décider de les faire évoluer, en fonction des demandes émanant de ses clients.

CPVP relève que les décisions que peut prendre la société excèdent « *l'espace de manœuvre normal* » caractéristique du champ d'action d'un sous-traitant. SWIFT a pris des « *décisions cruciales* » pendant cinq années dans le cadre de ses négociations secrètes avec le Département du Trésor américain.

L'absence de contact direct avec les personnes dont les données personnelles sont traitées, qu'invoque la société, ne permet pas d'écarter la qualification de responsable de traitement. Si les banques doivent effectivement être reconnues responsables du traitement, SWIFT en est le coresponsable selon la Commission. Cette dernière considère donc la société SWIFT SCRL comme responsable du traitement de données personnelles transitant par son système de communication SWIFTNet Fin.

La violation du droit européen du fait du fonctionnement ordinaire de SWIFTNet Fin

Une fois constatée l'applicabilité de la Directive aux activités de la société, la CPVP se prononce sur les éventuelles violations du texte communautaire en opérant une distinction entre deux situations : d'une part l'activité « ordinaire » de prestataire de service de messagerie aux clients au moyen de SWIFTNet Fin, d'autre part la transmission des données au Département du Trésor américain. Il est ainsi apparu que SWIFT ne remplissait pas toutes ses obligations légales, avant même que l'administration américaine ne lui ordonne de livrer ses données en 2001.

→ L'obligation d'informer les personnes dont les données sont traitées

L'article 11 de la Directive, transposé en droit belge à l'article 9 de la LVP, requiert des Etats membres qu'ils posent une obligation d'information à la charge du responsable de traitement, lorsque les données n'ont pas été collectées directement auprès de la personne concernée. Cette information doit être donnée « *dès l'enregistrement des données ou, si une communication à un tiers est envisagée, au plus tard lors de la première communication de données* »[90]. Cette obligation d'information porte sur l'identité du responsable de traitement et les finalités du traitement, ainsi que toute information supplémentaire « *nécessaire pour assurer à l'égard de la personne concernée un traitement loyal des données* »[91]. La Directive précise que la désignation des destinataires des données peut constituer une information nécessaire.

En l'espèce, il ne fait aucun doute que les personnes dont les données ont été collectées, c'est-à-dire les clients des banques, ont été informées de l'identité d'un responsable du traitement et de la finalité « initiale » du traitement. Du moins ont-ils été informés que les banques sont responsables du traitement de leurs données et que la finalité du traitement est l'exécution du contrat les liant à leur banque[92]. En revanche, ces clients n'ont pas été informés que SWIFT était coresponsable du traitement ni à quels tiers leurs informations étaient susceptibles d'être livrées.

La CPVP rejette ici l'argument de SWIFT selon lequel la société belge n'entretiendrait pas de relation directe avec les clients des banques du monde entier et n'aurait pas eu la possibilité de transmettre les informations requises. Les membres de la Commission considèrent en effet que l'obligation d'information aurait pu être remplie par l'intermédiaire

[90] Article 11 de la Directive.
[91] *Ibid.*
[92] Ces mesures d'information sont généralement posées par une clause contractuelle dans les conventions d'ouverture de compte bancaire.

des institutions financières elles-mêmes clientes de SWIFT. Ils concluent donc à la violation de l'obligation d'information transposée en droit belge, au regard de la « coresponsabilité » de SWIFT avec les institutions financières.

→ L'obligation de déclarer le traitement à l'autorité de protection des données personnelles

La Directive 95/46/CE impose aux Etats membres de mettre en place un système de publicité des traitements[93]. Les responsables de traitement doivent donc exécuter une obligation de déclaration ou de notification. Les formes de publicité requises peuvent varier selon la nature du traitement concerné et selon les choix opérés par chaque Etat lors de la transposition. En l'espèce, la loi belge imposait ici que la société SWIFT déclare le traitement SWIFTNet Fin à l'autorité de protection des données personnelles[94]. Or la société, si elle a déclaré certains des traitements dont elle est responsable, n'a pas déclaré ce traitement qui constitue l'essentiel de son activité[95]. La CPVP conclut donc à la violation de la LVP.

→ Le transfert des données collectées vers un pays ne présentant pas un niveau de protection adéquat

Le principe d'interdiction

Le transfert de données à caractère personnel vers un Etat dont le droit est considéré comme trop peu protecteur est en principe interdit par le droit européen[96]. La protection accordée par les règles communautaires et nationales pourrait en effet être contournée sans difficulté si les données pouvaient librement sortir du cadre juridique européen. Elles pourraient alors être utilisées indûment par des entités libérées des contraintes propres à la protection des données personnelles. Les règles protectrice doivent donc suivre les données en quelques mains qu'elles se trouvent, y compris hors d'Europe. Pour parvenir à ce résultat, des mécanismes originaux ont dû être élaborés afin de permettre une application extensive du droit européen, hors de l'Union européenne. Les différents mécanismes mis en place correspondent tous au même mécanisme : le transfert de données hors Union n'est possible que vers les Etats garantissant eux-mêmes un niveau de protection suffisant[97]. Ainsi le droit permet-il de créer une chaîne de protection des données. Les mécanismes dont il est question permettent de considérer que les données sont protégées en quelque lieu qu'elles se trouvent.

La Directive 95/46/CE exige que les pays tiers à l'Union européenne, vers lesquels un transfert de données à caractère personnel est envisagé, présentent un niveau de protection au moins « *adéquat* »[98]. Cette notion de niveau de protection adéquat est apparue en 1995 avec la Directive, qui précise que ce niveau s'apprécie « *au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données* ». « *Sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées* ». L'adéquation du niveau de protection est donc appréciée *in*

[93] Article 21 de la Directive.
[94] Conformément à l'article 17 de la LVP belge.
[95] Il est fait état d'un traitement des données nécessaires à la gestion des ressources humaines de la société, régulièrement déclaré à la CPVP.
[96] Article 25 de la Directive.
[97] Article 26 de la Directive.
[98] Article 25 de la Directive.

concreto, grâce à un faisceau d'indices permettant de rendre une image fidèle du respect de protection des données à caractère personnel. [99]

Le cas américain

Ces quelques développement pourraient paraître inutile tant il apparaît *a priori* évident qu'un pays comme les Etats-Unis porte une attention particulière à la protection des libertés fondamentales en général et au respect de la vie privée en particulier. Toutefois, ainsi que le rappelle la CPVP dans son avis, « *les Etats-Unis ne tombent pas dans la catégorie des pays présentant un niveau de protection adéquat* »[100]. La Commission européenne a en effet établi une « liste blanche » des pays offrant une protection adéquate[101] : cette liste comprend l'Argentine, le Canada, la Suisse ainsi que les îles Anglo-normandes (Ile de Man, Guernesey) mais exclut les Etats-Unis, pour plusieurs raisons qu'il convient de préciser.

Tout d'abord, le droit américain ne connaît pas de texte général protecteur des données personnelles qui serait comparable à la Directive 95/46/CE ou à une loi nationale comme la loi française Informatique, fichiers et libertés du 6 janvier 1978[102]. Au contraire, la protection des données personnelles résulte aux Etats-Unis de textes sectoriels, adoptés successivement dans des matières telles que la santé, l'éducation, la prospection commerciale ou encore les activités bancaires. De nombreuses activités ne sont donc pas contrôlées quant aux éventuelles atteintes aux données personnelles, les Etats-Unis refusant toute loi générale. Ils consentent en revanche à ce que les entreprises fassent le choix de se soumettre individuellement à un dispositif spécial de protection, les *Safe Harbor Principles*, que nous préciserons ultérieurement. Il convient toutefois de noter que l'administration américaine semble assez hostile à ce dispositif[103]. En outre, les Etats-Unis ne disposent pas d'une autorité de contrôle des données personnelles comparable aux autorités mises en place dans les Etats membres de l'Union européenne mais également dans nombre d'autres pays (Canada, Australie, Suisse…). S'il semble que le gouvernement Clinton ait projeté de créer une telle autorité, force est de constater que l'alternance républicaine et le déclenchement de la guerre contre le terrorisme ont causé un contexte peu propice à des avancées en la matière. Enfin, les Etats-Unis ne considèrent pas la protection des données personnelles comme un droit fondamental, malgré une tentative remarquée sur le fondement du Quatrième Amendement dans l'arrêt de la Cour suprême *United States v. Miller* (*cf supra*).

Pour ces raisons, la Commission européenne considère que les Etats-Unis ne disposent d'un système juridique garantissant un niveau de protection adéquat pour les transferts de données à caractère personnel.

Les exceptions au principe d'interdiction

---

[99] Sur toutes les questions relatives aux flux transfrontières de données, on pourra consulter le site internet de la conférence des 23-24 octobre 2006 organisé à Bruxelles par la Commission européenne.
<http://ec.europa.eu/justice_home/news/information_dossiers/conference_personal_data/interventions_en.htm>

[100] *Ibid.*, p. 19 de l'avis.

101 Commission européenne. « Décision de la Commission relative à la constatation du caractère adéquat de la protection des données dans les pays tiers » [en ligne]. Site internet de la Commission. Consultation le 14/06/07.
<http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_fr.htm>

[102] Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[103] L'intervention de Jean-Jacques Lavenue au 1er colloque sur le droit de l'administration électronique présente quelques traits de l'opinion de l'administration américaine en place sur le *Safe Harbor*.
LAVENUE Jean-Jacques. « Interopérabilité internationale, interconnexion des fichiers et protection des libertés : interrogation sur le devenir des données transférées dans le cadre de la lutte contre le terrorisme » in *Actes du 1er colloque sur le droit de l'administration électronique tenu à Paris les 6 et 7 décembre 2006.* [En ligne]. Site internet du colloque. Consultation le 10/06/07.
<http://dae2006.univ-paris1.fr/index.php?option=com_content&task=view&id=116&Itemid=50>

L'interdiction de transférer des données personnelles vers un pays ne présentant pas de telles garanties n'est toutefois pas absolue et il existe un certain nombre d'exceptions posées par l'article 26 de la Directive, pour les transferts rendus nécessaires par certains impératifs. Pour affirmer la légalité du transfert vers le serveur situé aux Etats-Unis, la société SWIFT considérait ainsi que les transferts vers son serveur américain étaient nécessaires :

- A l'exécution d'un contrat entre la personne concernée et le responsable du traitement
- A l'exécution d'un contrat entre le responsable du traitement et un tiers, dans l'intérêt de la personne concernée
- A la sauvegarde d'un intérêt public important

La CPVP a examiné successivement ces trois exceptions sans toutefois les retenir comme légitimant le transfert des données vers le serveur américain de la société. En premier lieu, la nécessité des transferts pour l'exécution d'un contrat entre le responsable du traitement et la personne concernée tout comme pour l'exécution d'un contrat dans l'intérêt de cette dernière est écartée par la Commission. La CPVP considère en effet que « *des alternatives et des services concurrents existent sur le marché des paiements internationaux* »[104] et donc que l'usage de SWIFTNet Fin n'était pas nécessaire à l'exécution des ordres de paiement des institutions financières. Il convient de noter que la Commission retient ici une vision extrêmement restrictive de la nécessité en l'assimilant à l'impossibilité absolue de recourir à un autre moyen. Au regard de la position quasi monopolistique de SWIFTNet Fin sur le marché de la messagerie interbancaire, la CPVP aurait sans doute pu admettre la nécessité en l'espèce. Le choix d'opérer une appréciation restrictive de l'exception est ici justifié par la volonté d'apprécier les dispositions de la Directive en faveur des personnes protégées. Les exceptions à l'interdiction de transférer des données vers un pays ne présentant pas un niveau de protection adéquat ne peuvent donc être interprétées que restrictivement.

En second lieu, la Commission rejette l'exception pour motif d'intérêt public important, invoquée par la société qui soutenait que la sauvegarde de l'ensemble de ses données sur le serveur américain visait à protéger la sécurité et la fiabilité du système financier dans son ensemble. La CPVP a en effet considéré que le risque d'une atteinte à l'ordre public belge n'était pas suffisant pour justifier l'installation d'un centre de traitement des données aux Etats-Unis.

Les solutions recommandées par la CPVP

Il est intéressant de noter qu'après avoir écarté les exceptions précitées, la Commission de la protection de la vie privée a pris la peine d'envisager trois mécanismes spécifiques susceptibles de garantir un traitement approprié des données aux Etats-Unis. Elle évoque ainsi les clauses contractuelles type, les règles d'entreprise contraignantes (ou *Binding Corporate Rules*) ainsi que les principes de la sphère de sécurité (ou *Safe Harbor Principles*). Or aucun de ces mécanismes n'était invoqué par SWIFT pour justifier le transfert des données vers son serveur américain et pour cause : la société n'a adhéré à aucun d'entre eux. La démarche de la CPVP consiste en réalité à examiner les différentes solutions qui pourraient être recommandées à SWIFT pour permettre à la société de transférer des données vers les Etats-Unis tout en respectant le droit européen des données personnelles. En se prononçant sur ces trois mécanismes, la Commission belge souhaite manifestement recommander à la société des manières de « régulariser » à l'avenir ses activités.

[104] *Ibid.*, p. 19 de l'avis.

Les clauses contractuelles types, stipulées dans le contrat liant le responsable de traitement et son sous-traitant, apportent une telle protection. La Commission européenne a approuvé trois modèles de clauses contractuelles types, consultables sur son site internet[105]. Il convient toutefois de noter que les clauses contractuelles types ont vocation à intervenir entre un responsable de traitement et un sous-traitant, ce qui n'est pas le cas en l'espèce, SWIFT n'étant pas considéré comme sous-traitant des banques.

Dans l'hypothèse où une même personne juridique remplit à la fois les fonctions de responsable de traitement et de sous-traitant, un code de conduite contraignant peut être adopté (*Binding corporate rules*) pour apporter des garanties suffisantes au regard de la protection des données. La vocation de telles règles, généralement adoptées par des sociétés commerciales, est d'offrir une norme interne de référence en matière de protection des données pour l'ensemble des entités d'un groupe international. Emises par la direction du groupe, elles contribuent à uniformiser les pratiques et à prévenir les risques inhérents aux traitements de données.

Enfin, le mécanisme de la sphère de sécurité (*Safe Harbor Principles*), spécifiquement élaboré pour les transferts de données vers les Etats-Unis, rendrait possible le transfert des données vers les Etats-Unis. Ce mécanisme repose sur l'adhésion volontaire des entreprises à des principes de protection des données, publiés par le Département du Commerce américain.

Nous étudierons ultérieurement les règles d'entreprise contraignantes et les principes de la sphère de sécurité, récemment adoptés par SWIFT (*cf infra*). Il n'en demeure pas moins que la CPVP, après avoir vérifié que la SWIFT n'avait à l'époque adhéré à aucun des trois mécanismes présentés ci-dessus, concluait en septembre 2006 à la violation de la LVP du fait du transfert de données personnelles bancaires vers un pays ne présentant pas un niveau de protection adéquat.

La violation du droit européen de la protection des données du fait de la livraison de données personnelles au Département du Trésor

Après avoir envisagé le transfert de données vers le serveur américain de la société SWIFT, il convient d'examiner plus précisément l'avis de la CPVP quant à ce qui constitue le cœur de l'Affaire SWIFT : la livraison de données au Département du Trésor.

→ La légitimité de principe du transfert au Département du Trésor

La CPVP, incompétente pour remettre en cause la validité des *subpoenas* prises en vertu du droit américain, se prononce en revanche sur la légitimité de la « livraison » des données par la société, au regard du droit européen. La Directive 95/46/CE, transposée en droit belge, dispose en effet que les traitements doivent être légitimes[106]. A cet égard, la société SWIFT invoque pour sa défense le caractère nécessaire du transfert des données, du fait du « *respect d'une obligation légale à laquelle le responsable du traitement est soumis* » ainsi que de « *la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées* »[107].

[105] Commission européenne. « Clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers » [en ligne]. Site internet de la Commission. Consultation le 14/06/07. <http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_fr.htm>

[106] Article 7 de la Directive

[107] *Ibid.*

S'agissant du respect des obligations légales auxquelles la société était soumise, c'est-à-dire de l'obéissance aux *subpoenas* adressées par le Département du Trésor, SWIFT a sur ce point développé une ligne de défense que l'on pourrait caricaturer comme une « politique du moindre mal », en tentant de démontrer qu'elle n'avait d'autre choix que de succomber aux prétentions de l'administration américaine. Obligée de se soumettre, la société aurait limité les atteintes à la vie privée en amenant l'administration américaine à accepter un encadrement de la livraison des données. L'accord secret conclu entre SWIFT et le Trésor aurait ainsi permis d'obtenir plusieurs mesures de protection[108] :

- Les données ne peuvent être requises qu'aux fins de lutte contre le terrorisme
- Seuls des ensembles limités de données peuvent être transmis, un accès illimité à la base de données ne pouvant être accordé
- SWIFT conserve un contrôle sur les données
- Les données transmises doivent être conservées dans des conditions propres à assurer leur sécurisation et leur confidentialité
- SWIFT dispose d'un droit de contrôle sur le respect de l'accord.

Il est intéressant de noter que la société soutient avoir agi ici dans le respect de ses règles internes en matière de *compliance*, c'est-à-dire de coopération avec les autorités de lutte contre les activités illégales. Il convient toutefois de noter que le respect par la société de ses règles internes ne préjuge en rien du respect des règles nationales et internationales applicables. La CPVP belge a donc repris la solution adoptée par le Groupe de l'article 29 dans le dossier des dispositifs d'alerte professionnels : si un responsable de traitement doit se soumettre aux obligations « *imposées par une loi ou un règlement étranger* », cette soumission ne peut avoir pour effet de contourner les règles protectrices du droit européen et de porter atteinte à la protection des données[109]. Cette opinion vaut d'autant plus le système juridique dont il est ici question ne présente pas un niveau de protection adéquat. La CPVP rejette donc le respect d'une obligation légale comme fondement du transfert au Département du Trésor.

S'agissant de l'intérêt légitime de SWIFT, la CPVP admet que l'intérêt de la société résidait manifestement dans la livraison de ses données au Trésor américain. En effet, ainsi que l'a démontré à de multiples reprises la société, elle se serait exposée à des sanctions en refusant d'exécuter les *subpoenas* délivrées par l'administration américaine. Pour surprenant que cela puisse paraître, la CPVP considère donc comme légitime le principe du transfert des données au Département du Trésor. En reconnaissant l'intérêt légitime de SWIFT à livrer ses données au Trésor, la CPVP n'a toutefois fait que constater qu'au regard du droit américain, la société avait effectivement tout intérêt à ne pas encourir des sanctions.

Il convient de noter que cette reconnaissance de principe s'imposait en réalité à la CPVP, qui ne pouvait reprocher à la société d'avoir respecté le droit américain sans prendre le risque de durcir le conflit entre les droits européen et américain. Pour condamner le programme secret SWIFT, la CPVP a donc préféré contester les conditions de transfert des données au Département du Trésor plutôt que son principe. C'est sans doute la raison pour laquelle la Commission estime finalement que « *les mesures exceptionnelles en vertu du droit*

---

[108] Commission à la protection de la vie privée canadienne. « Rapport de conclusions du 2 avril 2007 ». [En ligne]. Site internet de la Commission. Publication le 02/04/07. Consultation le 26/05/07 <http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_f.asp>

[109] Groupe de l'article 29. « Avis 1/2006 relatif à l'application des règles européennes de protection des données aux dispositifs internes d'alerte professionnelle ("whistleblowing") dans les domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières ». [En ligne]. Site internet de la Commission européenne. Publication le 01/02/06. Consultation le 07/05/07.
<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_fr.pdf>

américain pouvaient difficilement légitimer une violation cachée, systématique, massive et de longue durée des principes européens fondamentaux en matière de protection des données »[110].

→ Le défaut de proportionnalité dans la délivrance des données au Département du Trésor – La durée de leur conservation

La Directive 95/46/CE impose au responsable du traitement l'obligation de ne traiter que des données « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées* »[111]. Ces dispositions, transposées en droit belge dans la LVP, posent un principe général de nécessité et de proportionnalité des données collectées par rapport à la finalité du traitement.

Après avoir reconnu qu'il était dans l'intérêt légitime de SWIFT de se soumettre aux *subpoenas* américaine, la CPVP remet en cause cette reconnaissance en se fondant sur l'attitude de la société dans la conciliation des positions américaines et européennes. La Commission retient en effet une approche peu ordinaire du principe de proportionnalité : négligeant de relever la finalité du traitement et l'adéquation des données à cette finalité, la CPVP apprécie en premier lieu ce qu'elle qualifie de « *principe de nécessité* ». Elle considère en l'espèce que ce principe entraînait l'obligation pour la société SWIFT de concilier deux systèmes juridiques opposés.

Reconnaissant la situation délicate de la société, la CPVP considère néanmoins qu'il était du devoir de SWIFT de concilier les obligations qui s'imposaient à elle de part et d'autre en adoptant un comportement conforme aux deux positions. La Commission indique qu'auraient constitué un tel comportement la contestation des *subpoenas* devant les juridictions américaines ou encore l'application des procédures de collaboration judiciaire internationale. SWIFT n'ayant adopté aucun de ces deux comportements, la Commission considère avec sévérité que la société « *s'est limitée au respect du droit américain et à la recherche de solutions via des négociations secrètes avec l'UST*[112] ».

Ce n'est qu'après s'être prononcée sur ce principe de nécessité que la CPVP évoque – rapidement – le principe classique de proportionnalité. Elle rappelle à cet égard que le transfert de données vers le Département du Trésor est, selon elle, « *massif, caché durant depuis des années, et systématique* ». La société a donc violé le principe de proportionnalité en livrant des données excédant la finalité du traitement. Les *subpoenas* émises par le Département du Trésor, motivées en principe par la lutte contre le terrorisme, n'auraient dû viser que des personnes individuellement suspectées de terrorisme. Elles ne pouvaient avoir pour effet d'autoriser l'administration à consulter sans restriction la base de données de SWIFT, sauf à contraindre la société à violer le principe de proportionnalité. Il faut déduire de ces conclusions que la CPVP n'accorde pas de crédit aux affirmations de la société selon lesquelles seules des quantités limitées de données auraient été transmises au Département du Trésor.

Enfin, l'avis de la CPVP se prononce sur la durée de conservation des données par l'administration américaine. Les données doivent en effet être « *conservées […] pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement* »[113]. Aucun délai de

[110] p. 21 de l'avis.
[111] Article 6 de la Directive.
[112] *UST pour* « *United States Treasury* », traduit en français par Département du Trésor.
[113] Article 6 de la Directive.

conservation des données dans la boîte noire du Département du Trésor n'ayant été rapporté à la Commission, cette dernière considère ce délai comme indéterminé. Dès lors, l'absence de délai équivaut à un délai discrétionnaire, susceptible d'excéder la durée de conservation strictement nécessaire pour réaliser la finalité du traitement.

A défaut d'avoir respecté le principe de proportionnalité et la limitation du délai de conservation, la société SWIFT a donc violé le droit européen des données personnelles : « *en tant que responsable, [la société] aurait dû se rendre compte que ces principes étaient jugés fondamentaux dans l'ordre juridique européen* »[114]. Il est ainsi rappelé que la condamnation du comportement de SWIFT, fondé sur des principes juridiques, est avant tout fondée sur des principes européens. La société se voit donc reprocher d'avoir appliqué le droit américain plutôt que le droit européen des données personnelles.

→ L'obligation d'information à propos de la finalité du traitement

Le secret qui a entouré pendant cinq ans les accords passés entre SWIFT et l'administration américaine est sans doute l'une des causes prépondérantes du caractère polémique de l'Affaire SWIFT. C'est la raison pour laquelle la CPVP a souhaité porter une attention particulière aux obligations d'information à la charge de SWIFT. La finalité de lutte contre le terrorisme, si elle est reconnue par la CPVP, se trouve ainsi contestée en raison du défaut d'information des personnes concernées. La finalité bancaire initiale s'est en effet trouvée modifiée par l'ajout d'une finalité secrètement négociée entre SWIFT et le Département du Trésor.

Ce secret a interdit tout contrôle des autorités compétentes comme des personnes concernées, en contradiction avec l'obligation de définir la finalité du traitement[115] tout comme avec l'obligation d'information des personnes concernées[116]. Il est en effet apparu incertain que la finalité du traitement se limite strictement à la traque d'activités terroristes, cette incertitude résultant de l'absence de motivation explicite dans les *subpoenas* du Département du Trésor. Outre ces doutes quant à la finalité des demandes américaines, la CPVP reproche principalement à SWIFT d'avoir gardé secrète la délivrance de ses données.

Pour se défendre de ce défaut de transparence, la société a invoqué sans succès la confidentialité liée à ses activités de messagerie entre institutions financières, sensibles par nature. Cette recherche de confidentialité est attestée par la « politique de *compliance* » de SWIFT, qui définit les modalités de coopération de la société avec les autorités de lutte contre les activités illégales[117]. Elle comprend notamment une clause de « *no comment* », qui stipule que la nature sensible des contacts pris avec les autorités luttant contre les activités illégales implique que la société ne communique pas sur les demandes de ces autorités.

La Commission ne pouvait toutefois admettre que de simples règles internes à la société lui permettent d'échapper aux obligations posées par le droit belge et européen des données personnelles. L'obligation d'information imposée par la Directive et la LVP belge ne pouvait être mise en échec par les politiques internes de SWIFT. Les personnes concernées

[114] p. 23 de l'avis.
[115] Article 6 de la Directive.
[116] Article 10 de la Directive.
[117] SWIFT S.C.R.L. « *Statement on compliance* » [en ligne]. Site de la société. Consultation le 25/04/07. <http://www.swift.com/index.cfm?item_id=6149>.
La *compliance* peut se traduire comme un mécanisme de veille et de contrôle de la mise en conformité des pratiques d'une société avec la réglementation applicable.

auraient donc dû être informées de l'existence et de la finalité du traitement opéré par le Département du Trésor. La CPVP estime que SWIFT aurait au moins dû informer les institutions financières et les autorités de protection des données personnelles, au regard de l'ampleur des transferts exigés par l'administration américaine.

→ L'obligation de déclaration du transfert des données vers le Département du Trésor

La violation de cette obligation n'appelle pas de développements particuliers : la société SWIFT, qui n'a pas déclaré à la Commission son service SWIFTNet Fin – pourtant utilisé par les banques du monde entier – ne s'est évidemment pas risquée à déclarer le transfert de ses données vers le Département du Trésor. La Commission constate donc une nouvelle violation de la Directive 95/46/CE.

→ L'absence de contrôle indépendant sur le transfert de données

L'article 28 de la Directive, qui implique la création d'autorités de contrôle dans chaque Etat membre, impose qu'un mécanisme de contrôle indépendant permette de veiller au respect du droit européen des données à caractère personnel. Or le secret entourant le programme SWIFT a interdit, de fait, un quelconque contrôle sur le transfert de données à l'administration américaine. En empêchant à la Commission d'exercer ce contrôle indépendant, la société a donc une violé le droit européen des données personnelles.

Au vu des constatations que nous nous sommes efforcés d'expliciter, l'avis de la CPVP apparaît bien comme un document important de l'Affaire SWIFT. Il constitue le premier compte-rendu d'une enquête portant sur les aspects juridiques les plus délicats de l'Affaire. Il est également le document le plus consistant rendu en Europe par une autorité nationale de protection des données. Pour sa part, la Commission nationale de l'informatique et des libertés s'est contentée de quelques communiqués dénotant son peu d'implication dans la résolution de l'Affaire, les autres autorités nationales semblant avoir suivi la même ligne de conduite.

Malgré les multiples constats de violation du droit belge, européen et communautaire, nous verrons toutefois que les autorités politiques belges se sont fermement refusées à poursuivre la société SWIFT au-delà de la simple condamnation morale de son attitude. Nous constaterons également que l'Affaire, une fois rendues les conclusions des diverses enquêtes, est rapidement passée à une phase de négociation entre l'Union européenne et les Etats-Unis. Cette phase de négociation a largement relativisé le constat de violation du droit européen, *a fortiori* du droit belge. La CPVP s'est naturellement trouvée dépossédée de l'Affaire, du moins sur le plan international. Au contraire, elle a joué un rôle sur le plan national par le compromis qu'elle a obtenu de la société SWIFT. Nous verrons en effet que, parallèlement aux négociations internationales entre l'Union européenne et les Etats-Unis, la Commission belge a obtenu de SWIFT d'importantes mesures en faveur de la protection des données. Il convient enfin de réserver l'opinion de la CPVP quant à la responsabilité des institutions financières, que nous examinerons ultérieurement.

L'avis rendu par le Groupe de l'article 29 le 22 novembre 2006[118]

La Commission européenne s'est prononcée par la voix du Groupe de l'article 29 (G29), lequel a rendu un avis détaillé le 22 novembre 2006. La qualité du travail de la Commission de la protection de la vie privée belge est attestée par les conclusions du G29, pratiquement identiques à celles de la CPVP sur le fond du droit. Il n'apparaît pas nécessaire de reprendre ici l'argumentation suivi par le Groupe en ce qui concerne le constat des multiples violations de la Directive par la société SWIFT. Il convient toutefois de rappeler que le G29 se prononce strictement sur les violations de la Directive et non de la loi belge de transposition de cette même directive.

Le Groupe de l'article 29, créé par la Directive 95/46/CE pour veiller à l'application du texte, comprend des représentants des autorités nationales de protection des données personnelles afin de mieux coordonner l'action communautaire en la matière. Se référant exclusivement à la Directive, elle exprime ainsi la voix de l'Europe sans faire référence aux spécificités nationales. Nous verrons que son avis a été précieux dans le dialogue instauré entre l'Union européenne et les Etats-Unis pour dénouer le conflit né de l'Affaire SWIFT.

L'avis du 22 novembre 2006, à la différence de celui rendu par la CPVP belge, s'achève sur les « *mesures à adopter dans l'immédiat pour redresser la situation actuelle* »[119]. Ces mesures, qui constituent un véritable guide de conduite à destination des différents acteurs de l'Affaire, recommandent à SWIFT et aux institutions financières de régulariser les traitements de données dont ils sont responsables. Il est notamment préconisé que les banques centrales européennes clarifient leur mandat de surveillance sur la société SWIFT et que les institutions financières informent leurs clients de l'existence du système SWIFT mais aussi de l'éventualité que les autorités américaines accèdent à leurs données.

S'agissant de l'opinion du Groupe quant à la responsabilité des banques et des autres institutions financières mises en cause dans l'Affaire, nous l'examinerons conjointement à celle de la CPVP (*cf infra*).

L'avis rendu par le Contrôleur européen de la protection des données le 1er février 2007[120]

Le Contrôleur européen de la protection des données (CEPD), en fonction depuis 2004, est chargé de veiller au respect des données personnelles au sein des institutions communautaires[121]. Il joue ainsi un rôle proche de celui des autorités nationales de protection des données, mais au niveau communautaire. La Banque centrale européenne (BCE) est l'un de ces organes et se trouve donc dans son champ de compétence.

---

[118] Groupe de l'article 29. « Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) ». [En ligne]. Site internet de la Commission européenne. Publication le 22/11/06. Consultation le 05/01/07.
Cet avis a fait l'objet d'un commentaire de CAPRIOLI Eric A., « Violation des règles propres aux données à caractère personnel et réseau SWIFT », in *Revue de droit bancaire et financier*, janvier-février 2007.
<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf>

[119] *Ibid.* p. 30.

[120] Contrôleur européen de la protection des données. « Avis du CEPD sur le rôle de la Banque centrale européenne dans l'affaire SWIFT ». [En ligne]. Site internet du Contrôleur. Publication le 01/02/07. Consultation le 10/03/07.
<http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2007/07-02-01_Opinion_ECB_role_SWIFT_FR.pdf>

[121] Site internet du CPED
<http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/pid/1>

L'actuel CEPD – Peter Hustinx – avait émis une première opinion le 4 octobre 2006 sur le rôle de la BCE dans l'Affaire SWIFT[122]. Cette opinion, qui approuvait les conclusions de la CPVP du 27 septembre 2006, reprochait à la BCE de n'être pas intervenue pour empêcher SWIFT de transférer des données à caractère personnel aux autorités américaines et de s'être abstenue de dénoncer le programme secret aux gouvernements et autorités européennes.

Dans un avis du 1er février 2007, le CEPD s'est prononcé plus spécifiquement sur le rôle de la BCE[123]. Nous examinerons cet avis dans le cadre de l'étude des mesures prises par les institutions financières suite à l'Affaire SWIFT (*cf infra*). En effet, à ce stade, il n'est plus question d'une réaction immédiate aux révélations de la presse américaine mais bien de la résolution de l'Affaire. Il convient néanmoins de noter d'ores et déjà que cet avis a permis de fixer les responsabilités de la BCE, question qui n'avait été qu'effleurée par la CPVP et le Groupe de l'article 29. La responsabilité des institutions bancaires est en effet importante dans l'Affaire SWIFT, ces dernières s'étant abstenues de dénoncer le programme américain aux autorités européennes.

Des enquêtes non suivies de sanctions

Il convient de noter que, parmi toutes les enquêtes envisagées immédiatement après les révélations du *New York Times*, certaines ont été menées dans une grande confusion. Il n'est donc pas étonnant qu'elles n'aient pas toutes abouti. Les enquêtes administratives évoquées par certains Etats membres, à supposer qu'elles aient été effectivement menées, ne semblent pas avoir fait l'objet d'une quelconque publicité. Quant à celles qui ont été menées à bien et publiées, leur dénouement a pu paraître déconcertant aux yeux des observateurs : la reconnaissance de l'existence du programme SWIFT et, le plus souvent, de son illégalité, ne s'est nulle part accompagnée de sanctions.

Cette absence de sanctions a largement contribué au sentiment d'un déséquilibre dans les rapports entre les Etats-Unis et l'Union européenne, l'un imposant ses volontés à l'autre. On trouve ainsi de nombreuses réactions, notamment sur des blogs spécialisés dans la protection des droits fondamentaux, pour regretter que la dénonciation du programme secret ne s'accompagne pas de mises en cause de la responsabilité des parties condamnées pour violation du droit européen et national des données personnelles[124]. La presse s'est faite le relais de cette déception qui dénote une certaine frustration quant à l'efficacité du droit européen[125].

---

[122] Contrôleur européen de la protection des données. « SWIFT : Premières conclusions du CEPD sur le rôle de la BCE ». [En ligne]. Site internet du Contrôleur. Publication le 04/10/06. Consultation le 08/03/07. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2006/EDPS-2006-10-FR_swift.pdf>

[123] Contrôleur européen de la protection des données. « Avis du CEPD sur le rôle de la Banque centrale européenne dans l'affaire SWIFT ». [En ligne]. Site internet du Contrôleur. Publication le 01/02/07. Consultation le 10/03/07. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2007/07-02-01_Opinion_ECB_role_SWIFT_FR.pdf>

[124] Le Blog du Kazz. « Affaire Swift : rien n'a changé, sauf qu'on sait ». [En ligne]. Blog de l'auteur. Publication le 12/02/07. Consultation le 13/05/07. <http://kazz9.ovh.org/kazz/blog/index.php?2007/02/13/31-swift-protection-donnees-personnelles-g29-cnil-europol>

[125] M. Bu. « Vous êtes en faute, surtout continuez ». [En ligne]. Site internet du journal La Libre Belgique. Publication le 29/09/06. Consultation le 19/06/07. < http://www.lalibre.be/article.phtml?id=10&subid=91&art_id=308235>

En effet, les tenants de l'opinion européenne vont rapidement faire le choix de la conciliation plutôt que celui de la sanction, en profitant cependant d'un net avantage dans la négociation du fait de la large réprobation suscitée par le programme américain.

Euronews. « Le dossier Swift classé sans suites par la justice belge ». Cité par Spyworld.com. [En ligne]. Publication le 13/12/06. Consultation le 10/05/07.
<http://www.spyworld-actu.com/spip.php?article3237>
ROZENFELD, Sylvie. « Swift : condamnation sans sanction ». Expertises janvier 2007. p.3.

Seconde partie : Le maintien du programme dans le respect du droit européen

L'Affaire SWIFT met en cause des intérêts fondamentaux et des parties éminentes. Son caractère politique autant qu'international désignait naturellement les autorités européennes et américaines pour résoudre un conflit qui paraissait insoluble. Une intervention strictement judiciaire étant exclue, la résolution passait donc par des négociations directes entre l'Union européenne et les Etats-Unis **(A)**. Il n'en demeure pas moins que le secteur financier, considéré comme responsable par les autorités européennes, a dû faire évoluer ses pratiques pour améliorer sa transparence et son respect des données personnelles. SWIFT comme les institutions financières ont ainsi pris des mesures importantes qui marquent la prise de conscience par le secteur de son rôle dans la protection des données **(B)**.

Chapitre I : L'engagement américain résultant des négociations avec l'Union européenne

Sur le plan politique, la résolution du conflit passait nécessairement par des négociations entre l'Union européenne et les Etats-Unis. Ces négociations, fondées sur les conclusions des enquêtes menées par les autorités européennes, se sont déroulées à Washington et ont permis aux parties de faire entendre leurs préoccupations mais aussi de rechercher un compromis **(1)**. L'accord finalement conclu prend la forme d'un simple engagement unilatéral américain, qui offre toutefois des garanties exceptionnelles à l'Union européenne jusque sur le territoire américain **(2)**.

Section I : La préparation et le déroulement des négociations entre l'Union européenne et les Etats-Unis

L'inadéquation de poursuites judiciaires – Le choix de la négociation

Après avoir envisagé l'opposition entre les systèmes juridiques européen et américain, il s'agit d'examiner de quelle manière le conflit noué autour du transfert secret de données bancaires a pu être résolu sur le plan politique. Dans l'Affaire SWIFT, l'opposition entre Etats-Unis et Union européenne se cristallisait autour d'une question de droit. Elle semblait donc appeler une réponse juridique à la question de la violation du droit européen. Comment imaginer toutefois qu'un juge, qu'il soit américain ou européen, tranche le litige ? Comment concevoir que le respect des intérêts en présence passe par une décision juridique univoque, tant ces intérêts sont opposés ?

A cet égard, sans doute faut-il tout d'abord relever que l'Affaire SWIFT présente un caractère éminemment politique[126]. Il serait donc réducteur de la considérer comme une

[126] POULLET Yves et DEGRAVE Elise. « L'Affaire SWIFT » in *Revue du Droit des Technologies de l'Information* n° 27, 2007. Cet article est disponible en ligne sur le site internet du Parlement européen. Consultation le 02/03/07.
<http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/poullet_degrave_/poullet_degrave_fr.pdf>

simple question de violation de la protection des données personnelles. Intervenant dans un contexte de relations tendues entre l'Union européenne et les Etats-Unis, elle renvoie dos-à-dos les parties, tant leurs préoccupations respectives sont différentes. Il ne s'agit donc pas ici d'une « simple » question juridique. Ce caractère éminemment politique excluait donc une intervention judiciaire dans la résolution du conflit. Outre qu'elle n'aurait pas permis de trancher le litige, une action judiciaire aurait sans doute été maladroite. Certes, le constat de violation du droit des données personnelles par les autorités européennes, susceptible de se prolonger par la saisine des juridictions compétentes, aurait permis de sanctionner la société SWIFT ou les institutions bancaires. Toutefois, vu la sensibilité du dossier et l'importance des intérêts en présence, une décision judiciaire à l'encontre de SWIFT n'aurait fait que placer la société dans une situation difficile, sans atteindre l'administration américaine.

L'engagement de la responsabilité de SWIFT ou des institutions financières n'aurait sans doute fait que détourner le débat des véritables parties de l'Affaire, en perturbant le dialogue avec le principal responsable du programme secret SWIFT, c'est-à-dire le Département du Trésor américain. Une telle action aurait pu être perçue comme une marque d'unilatéralisme, peu propre à dénouer le conflit entre les Etats-Unis et l'Europe quant aux moyens de lutter contre le terrorisme.

Enfin, il n'est pas besoin de développer les principes du droit international public pour rappeler, de manière caricaturale, que les Etats souverains ne sont soumis au droit que dans la mesure où ils l'acceptent. Dès lors, il est apparu impossible de condamner judiciairement les Etats-Unis pour la violation du droit européen et la résolution du conflit passait nécessairement par une phase de concertation.

Encore faut-il préciser que les enjeux de la négociation ont largement débordé du débat entre sécurité et liberté, souvent teinté de manichéisme: nombre d'observateurs ont en effet relevé que le transfert des données de SWIFT pourrait être d'une grande utilité en termes d'espionnage économique et de surveillance des activités financières, hors de tout contexte terroriste[127]. Il a donc fallu négocier, directement avec l'administration américaine, afin de parvenir à une entente. La société SWIFT a soutenu ces négociations[128] : outre qu'elles étaient susceptibles de résoudre le conflit tiraillant la société entre deux forces contraires, de telles tractations politiques ont sans doute permis de minimiser le rôle joué par la société dans le déroulement de l'Affaire.

---

[127] Pour un exemple de ces craintes, lire l'opinion de la CNIL rapportée par le journal Innovation :
BOLLE William. « Affaire Swift : la CNIL veut contrer la CIA ». [En ligne]. Site internet du journal Innovation. Publication le 13/06/07. Consultation le 19/07/07.
<http://www.innovationlejournal.fr/spip.php?article650>
Avec une plus grande prudence, on pourra consulter :
CARON Pierre. « La guerre électronique n'aura pas lieu ». [En ligne]. Site internet Knowckers. Publication le 04/12/06. Consultation le 25/06/07.
<http://www.knowckers.org/index.php?option=com_content&task=view&id=218&Itemid=0>

[128] SWIFT SCRL. « SWIFT appuie l'appel à des négociations entre l'Europe et les Etats-Unis sur la sécurité et la protection des données privées». [En ligne]. Site internet de la société. Publication le 28/09/06. Consultation le 01/05/07.
<http://www.swift.com/index.cfm?item_id=60653>

La désignation naturelle des institutions communautaires pour négocier face aux Etats-Unis

Le choix d'une résolution politique s'est imposé en quelques mois, pour les raisons que nous avons évoquées. Il restait toutefois à déterminer les parties à la négociation.

Alors que les autorités nationales de protection des données ont vivement réagi face au programme SWIFT, plus ou moins soutenues dans la dénonciation de l'action de l'administration américaine, il convient de s'interroger sur les raisons ayant amené l'Union européenne à se saisir du dossier, jusqu'à en déposséder les autorités nationales des Etats membres. Si l'Affaire SWIFT présente de nombreux points de rattachement au territoire et à la juridiction belge, elle s'étend bien au-delà des frontières d'un territoire national.

On a toutefois pu imaginer que les autorités politiques nationales prennent en charge ces négociations individuellement, dans le cadre de négociations bilatérales avec les Etats-Unis. De telles négociations auraient naturellement fait suite aux enquêtes des autorités nationales de protection des données (dont la CPVP belge), mais auraient sans doute fragilisé la position européenne face aux autorités américaines. En effet, les Etats membres de l'Union ne disposaient pas tous d'informations suffisantes pour entrer dans de telles négociations. En outre, il ne peut être exclu que certains d'entre eux auraient préféré rester prudemment à l'écart d'un « bras de fer » tendu avec le gouvernement américain.

Il convient également de remarquer que les droits nationaux des données personnelles, harmonisés lors de la transposition de la Directive 95/46/CE, continuent de présenter quelques différences techniques selon les Etats membres. Pour éviter de devoir traiter spécifiquement chaque conflit qui se serait posé avec le droit américain, il était naturel de se référer à la Directive – dénominateur commun des législations européennes en la matière – et de confier la résolution du conflit à l'organisation ayant élaboré la Directive.

Il est donc apparu raisonnable de confier la défense d'une position européenne commune aux organes communautaires, qui étaient sans doute les mieux « armés » pour négocier un accord satisfaisant avec les Etats-Unis. Une intervention de l'Union européenne est présumée avoir plus de poids que des initiatives individuelles de la part des Etats membres. En outre, les organes communautaires semblaient désignés pour résoudre ce conflit international par nature : l'Affaire SWIFT porte sur une violation du droit européen des données personnelles par une société coopérative belge qui, conformément à des injonctions administratives américaines, a livré des données bancaires de clients du monde entier. Le caractère international de l'Affaire impose ainsi une résolution du conflit au-delà des frontières nationales. Il justifie que l'Union européenne ait occupé l'espace de négociation face aux Etats-Unis et nous examinerons le rôle joué par les différents organes communautaires dans la négociation.

Les deux caractères fondamentaux de l'Affaire SWIFT – ses implications internationales ainsi que la nécessité d'une solution politique – désignaient donc l'Union européenne comme partenaire des Etats-Unis dans la négociation d'une solution propre à ménager les intérêts de chaque partie.

La préparation des négociations par les organes communautaires

Plusieurs institutions communautaires étant intervenues dans les négociations, il convient de préciser leurs rôles respectifs avant d'examiner la position américaine. A cet égard, on peut considérer qu'aussitôt passées les premières réactions nationales et

européennes à la révélation du programme, les institutions communautaires se sont attelées à la conciliation des intérêts en présence.

Ainsi le Parlement européen prévoyait-il, dès le 6 juillet 2006[129], l'organisation d'une audition par sa commission des libertés civiles et sa commission des affaires économiques[130]. Le 4 octobre 2006, ces deux commissions ont ainsi entendu conjointement le directeur financier de la société SWIFT, le président de la Banque centrale européenne, des représentants de la Banque nationale de Belgique, un représentant du Groupe de l'article 29, un membre de la Commission européenne, le Contrôleur européen de la protection des données ainsi que la présidente du Sénat belge[131]. Le Conseil européen, invité à s'exprimer sur l'Affaire, n'envoie aucun représentant à cette audition. Cette absence remarquée sera d'ailleurs vivement regrettée par les présidents des commissions[132].

Il ressort de ces auditions que les données de SWIFT sont dupliquées sur un serveur situé aux Etats-Unis afin de constituer une base de données de sauvegarde des données (*back-up*) utile en cas de défaillance du système. La localisation du serveur sur le territoire américain soumet les données conservées au droit américain et permet à l'administration américaine d'enjoindre à SWIFT de livrer les données requises. La présidente du Sénat belge, après avoir rappelé l'illégalité du comportement de SWIFT et des institutions bancaires, a conclu à la nécessité d'« *établir un cadre (euro-américain) pour en finir avec les divergences* »[133]. De nombreux appels en ce sens, dont ceux de la société SWIFT elle-même, amènent le Parlement à entrer pleinement dans la phase de négociation. Son intervention passera notamment par l'organisation de conférences sur les questions posées par l'Affaire[134], ponctuées par des résolutions marquant la volonté des eurodéputés de suivre l'avancement des tractations.

De son côté, la Commission organise à Bruxelles une conférence sur les transferts internationaux de données à caractère personnel les 23 et 24 octobre 2006[135]. Participent à cette conférence le Groupe de l'article 29 mais aussi le Département du Commerce américain, chargé par les Etats-Unis de négocier les conditions de ces transferts. Si elle ne porte pas

---

[129] Parlement européen. « Résolution du Parlement européen sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains ». [En ligne]. Site internet du Parlement. Publication le 06/07/06. Consultation le 04/03/07.
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0317+0+DOC+XML+V0//FR>
Le paragraphe 13 de la résolution prévoit l'audition des acteurs de l'affaire.

[130] Le site de la commission des libertés civiles, de la justice et des affaires intérieures :
<http://www.europarl.europa.eu/committees/libe_home_fr.htm>
Le site de la commission des affaires économiques et monétaires :
<http://www.europarl.europa.eu/committees/econ_home_fr.htm>

[131] Toutes les contributions à l'audition du 4 octobre 2006 sont disponibles sur le site du Parlement européen, dans la rubrique des auditions publiques. Elle est accessible en ligne à l'adresse suivante :
<http://www.europarl.europa.eu/hearings/2006_fr.htm>

[132] Parlement européen. « Question orale posée par Pervenche Berès, au nom de la commission des affaires économiques et monétaires, Jean-Marie Cavada, au nom de la commission des libertés civiles, de la justice et des affaires intérieures au Conseil ». [En ligne]. Site internet du Parlement. Publication le 21/12/07. Mise à jour le 08/01/07. Consultation le 20/03/07.
<http://www.europarl.europa.eu/sides/getDoc.do?type=OQ&reference=O-2006-0131&language=FR>

[133] Présidence du Sénat de Belgique. « La transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de US Treasury Department (OFAC) – Exposé du 4 octobre 2006 au Parlement européen ». [En ligne]. Publication le 04/10/06. Consultation le 27/03/07.
<http://www.senaat.be/event/20061004-swift/Texte-Lizin-EP-F.doc>

[134] Voir note 119.

[135] Commission européenne. « Conférence sur les transferts internationaux de données personnelles ». [En ligne]. Publication octobre 2006. Consultation le 19/04/07.
<http://ec.europa.eu/justice_home/news/information_dossiers/conference_personal_data/index_en.htm>

exclusivement sur l'Affaire SWIFT, la conférence permet de mener une réflexion sur les possibilités de garantir un niveau de protection adéquat aux données transférées hors de l'Union européenne. Sont ainsi étudiés, dans divers ateliers de réflexion, les principes du *Safe Harbor*, les clauses contractuelles types ainsi que les règles d'entreprise contraignantes.

Le 31 janvier 2007, le Parlement européen débat des PNR et de l'Affaire SWIFT[136]. Ce débat marque l'attachement renouvelé des députés à faire respecter les libertés mais aussi la souveraineté européenne[137]. Jean-Marie Cavada, président de la commission des libertés civiles, s'insurge à cette occasion de l'attitude américaine et indique que ne sont pas seulement en jeu les droits fondamentaux des citoyens européens, mais également « *la crédibilité du partenariat avec les Etats-Unis* ». Il critique ouvertement la distance prise par le Conseil européen à l'égard du dossier. Martine Roure, du parti socialiste européen (PSE), souligne « *le besoin urgent de définir un cadre global pour la transmission et la protection des données personnelles dans le cadre des relations transatlantiques* ».

Le député Alexander Radwan, du parti populaire européen (PPE), propose que les négociations soient entamées dans le cadre du G7, l'Allemagne occupant à la fois la présidence du Conseil européen et de cette réunion. Cette proposition, reprise par plusieurs députés, est toutefois accueillie avec circonspection par le président en exercice du Conseil de l'Union, Günter Gloser. Ce dernier considère que, dans l'hypothèse où les données seraient effectivement conservées par SWIFT aux Etats-Unis, l'Union européenne « *ne pourrait exercer la moindre influence* ». Les débats indiquent clairement que le Conseil et la Commission préfèrent adopter une attitude excessivement prudente, rappelant à de multiples reprises la nécessité de concilier la protection des données avec la lutte contre le terrorisme. Le vice-président de la Commission européenne va ainsi jusqu'à exprimer des réserves sur la publicité qui pourrait être donnée à un accord entre les Etats-Unis et l'Union européenne au terme de l'Affaire SWIFT. Cette publicité serait, selon lui, susceptible « *d'offrir un puissant outil aux personnes suspectées de terrorisme* ». Il est surprenant de lire que le commissaire Frattini emploie ici un argument invoqué par l'administration américaine pour regretter la révélation du programme secret. Pour se convaincre de la prudence de la Commission, il n'est que de lire la conclusion du commissaire qui martèle que « *le problème, ce sont les terroristes, et non les Etats-Unis* ». Ces déclarations du Conseil et de la Commission européenne seront vivement critiquées par le groupe gauche unitaire européenne (GUE) dans les déclarations écrites des députés Guerreiro et Pafilis, consignées aux débats.

Ce débat a été suivi d'une résolution sur le dialogue transatlantique, votée par le Parlement le 14 février 2007[138]. Prenant acte de la volonté de négocier exprimée par l'administration américaine, le Parlement souhaite que la question des données personnelles soit abordée lors du sommet Union européenne – Etats-Unis du 30 avril 2007[139]. Les députés

---

[136] Parlement européen. « Débat sur le nouvel accord 'PNR' – SWIFT ». [En ligne]. Site internet du Parlement. Publication le 31/01/07. Mise à jour le 04/04/07. Consultation le 10/05/07. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20070131+ITEM-019+DOC+XML+V0//FR&language=FR>

[137] A noter que le président de la commission des libertés civiles du Parlement européen, Jean-Marie CAVADA, a soulevé à plusieurs reprises ces questions pour regretter que la souveraineté européenne ne soit pas mieux défendue par les organes communautaires (dont le Conseil européen) et qu'elle soit mise à mal par les Etats-Unis.

[138] Parlement européen. « Résolution du Parlement européen sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions ». [En ligne]. Site internet du Parlement. Publication le 14/02/07. Mise à jour le 01/08/07. Consultation le 06/08/07. <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0039&language=FR&ring=B6-2007-0042>

[139] Paragraphe 12 de la résolution.

insistent alors sur la volonté d'être associés à ces négociations. La résolution présente les exigences de la position européenne : « *SWIFT devrait mettre un terme à sa pratique actuelle de reproduire toutes les données concernant des citoyens et entreprises de l'Union européenne sur son site miroir ou installer l'autre site de sa base de données en un lieu qui n'est pas sous la souveraineté américaine* ». Le Parlement encourage l'adhésion des entreprises européennes exerçant des activités aux Etats-Unis aux principes du *Safe Harbor*[140]. En outre, la Commission européenne est invitée à analyser les risques d'espionnage économique et commercial au moyen du système SWIFT[141].

Le 26 mars 2007, le Parlement organise à Bruxelles un séminaire public sur les PNR, Swift et le *Safe Harbor*[142]. Ce séminaire constitue un socle de réflexion pour les négociateurs européens qui doivent rencontrer les représentants américains un mois plus tard. Organisé par la commission des libertés civiles, il porte précisément sur les sujets qui seront négociés en avril aux Etats-Unis. Le 25 avril 2007, une résolution rappelle la volonté du Parlement de participer davantage aux négociations transatlantiques, à cinq jours des négociations qui se tiendront le 30 à Washington[143].

La délégation de la Commission européenne envoyée à Washington pour négocier avec le Département du Trésor comprenait Franco Frattini, vice président de la Commission ainsi que Peer Steinbrück, ministre des Finances allemand et représentant du Conseil européen. Elle a obtenu de la part des Etats- Unis un engagement unilatéral que nous aurons l'occasion de développer (*cf infra*).

Le 21 juin 2007, le Parlement rappelle sa volonté que soit conclu un accord international afin d'assurer la conformité du système SWIFT à la directive 95/46/CE[144]. Cet accord doit prévoir « *les garanties nécessaires contre toute utilisation abusive des données à des fins économiques et commerciales* ». Nous verrons que la solution du conflit est passée par un outil juridique unilatéral, moins contraignant que l'accord bilatéral appelé de ses vœux par le Parlement européen.

La position américaine dans les négociations

L'administration américaine n'a eu de cesse de mettre en avant l'efficacité de son programme de collecte des données bancaires destiné à la lutte contre le terrorisme. Elle a rappelé, tout au long de l'Affaire, son attachement à ce programme qui aurait permis de mener à bien des poursuites contre des terroristes extrêmement dangereux. La position américaine sur le sujet est claire : le programme de pistage du financement du terrorisme « *sauve des*

[140] Paragraphes 21 et 24 de la résolution.
[141] Paragraphe 23 de la résolution.
[142] Parlement européen. « Programme du séminaire 'PNR/SWIFT/Safe Harbour – Les données transatlantiques sont-elles protégées ?' ». [En ligne]. Site internet du Parlement. Publication mars 2007. Consultation le 27/05/07. < http://www.europarl.europa.eu/hearings/20070326/libe/programme_en.pdf>
[143] Parlement européen. « Résolution du Parlement européen sur les relations transatlantiques ». [En ligne]. Site internet du Parlement. Publication le 25/04/07. Mise à jour le 09/05/07. Consultation le 07/06/07. <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0155&language=FR&ring=B6-2007-0156>
[144] Parlement européen. « Résolution du Parlement européen sur l'espace de liberté, de sécurité et de justice: stratégie sur la dimension extérieure, plan d'action mettant en œuvre le programme de La Haye». [En ligne]. Site internet du Parlement. Publication le 21/06/07. Mise à jour le 29/06/07. Consultation le 05/07/07. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0284+0+DOC+XML+V0//FR>

vies ». Il n'est donc jamais apparu dans la rhétorique américaine que la cessation du transfert des données au Département du Trésor était une option envisageable.

Au-delà, le gouvernement a pris soin de souligner la conformité du programme avec le droit américain et au contraire d'éviter d'évoquer la violation du droit européen. A lire et à entendre les responsables américains concernés, cette seconde question semble même ne pas se poser.

Les négociateurs américains ont ainsi imposé une marge de manœuvre assez réduite à leurs interlocuteurs européens : en acceptant la négociation, les Etats-Unis ont manifesté leur volonté de faire un geste vers l'Europe en consentant des garanties supplémentaires au regard de la protection des données personnelles, sans que ce geste aille jusqu'à remettre en cause l'existence et la persistance du programme SWIFT. Cette marge de négociation apparaît clairement à la lecture de la note envoyée le 28 juin 2007 par le Département du Trésor à la Commission et au Conseil européen[145], qui récapitule la conception américaine de la lutte contre le terrorisme.

Le cadre général des négociations entre l'Union européenne et les Etats-Unis

Après avoir présenté les principales parties à la négociation et leurs prétentions, il convient de préciser les diverses solutions envisagées pour dénouer le conflit.

Les documents échangés lors des tractations sont difficiles à obtenir en raison de la confidentialité qui entoure les négociations internationales. Dès lors, nous nous réfèrerons aux documents antérieurs et postérieurs à la négociation, qui exposent les positions européenne et américaine ainsi que les concessions proposées par chaque partie. Nous envisagerons tout d'abord les différentes solutions avant d'examiner la forme et le fond de la résolution des négociations (*cf infra*).

Le choix de la négociation impliquait la recherche de concessions réciproques. Or la première solution envisagée, la plus radicale sans doute, était celle recommandée dans un premier temps par les institutions européennes. Cette solution, qui aurait naturellement résulté du constat de violation du droit européen, aurait été la cessation immédiate des transferts exigés par l'administration américaine. Cette position est toutefois apparue inacceptable pour les négociateurs américains. En effet, au regard du droit américain, le programme secret SWIFT est légal. Dès lors, les négociations ne pouvaient s'orienter vers un accord sans offrir de contrepartie aux Etats-Unis. La cessation des transferts a donc été rapidement écartée car trop difficile à négocier, l'administration américaine tenant à conserver un outil déterminant dans la guerre contre le terrorisme. Les négociateurs européens ont donc dû composer avec cet impératif et les négociations se sont donc orientées vers la recherche des garanties les plus à même de remplir cet objectif.

---

[145] Département du Trésor. « Traitement par le département du Trésor des États-Unis, aux fins de la lutte contre le terrorisme, de données à caractère personnel provenant de l'UE — «SWIFT» ». [En ligne]. Site de l'accès au droit de l'Union européenne. Publication le 20/07/07. Consultation le 08/08/07. <http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2007/c_166/c_16620070720fr00170017.pdf>

Section II : Le résultat des négociations : un engagement unilatéral de la part du gouvernement américain

Les garanties accordées unilatéralement par le Département du Trésor

Alors que SWIFT s'engage à respecter une plus grande transparence et adhère au *Safe Harbor* (*cf infra*), la Commission et le Conseil européen poursuivent les négociations avec les autorités américaines pour obtenir des engagements de l'administration. Les négociations menées en avril 2007 à Washington aboutissent et permettent d'obtenir un engagement unilatéral du Département du Trésor. En effet, plutôt que de prévoir un accord international, instrument juridique nécessitant une organisation assez lourde, l'administration américaine a préféré donner à son engagement une forme unilatérale. Une lettre du Département du Trésor du 28 juin 2007, signée par le Sous-secrétaire du Trésor en charge du terrorisme et du renseignement financier Stuart A. Levey et adressée à la Commission et au Conseil européen, exprime cet engagement. Publiée au Journal officiel des Communautés européennes, elle est accompagnée d'« observations » qui présentent l'opinion américaine sur l'Affaire SWIFT ainsi que les garanties consenties par les autorités américaines comme contrepartie à l'acceptation par l'Union européenne de la continuation du transfert de données vers le Département du Trésor[146]. Ces observations comprennent les engagements suivants :

- Le Département du Trésor n'utilisera les données de la société SWIFT que pour lutter contre le terrorisme, y compris lorsqu'il sera amené à transférer ces données à d'autres agences américaines ou à des pays tiers. Les données ne pourront être utilisées à d'autres fins. Cet engagement répond aux inquiétudes européennes quant à la finalité de l'extraction des données par le Département du Trésor. Il garantit que seule la lutte contre le terrorisme est susceptible de motiver les demandes de l'administration, à l'exclusion de toute finalité économique ou d'espionnage.

- Les données reçues seront analysées en permanence afin d'effacer toute donnée non nécessaire à la lutte contre le terrorisme. Cette garantie est assez proche de celle consentie à SWIFT lors de la négociation de l'accord secret entre la société et l'administration américaine. Ce contrôle apparaît toutefois comme plus systématique et correspond aux exigences européennes d'adéquation des données à la finalité du traitement. Ainsi, toutes les données inutiles – ou devenues inutiles – doivent être supprimées de la base de données du Département du Trésor.

- Les données obtenues ne seront pas conservées plus de cinq années à compter de leur réception si elles s'avèrent inutile à la finalité de lutte contre le terrorisme. L'engagement américain de supprimer les données inutiles s'accompagne ici d'un seuil limite de conservation, qui impose à l'administration de supprimer automatiquement toute donnée conservée au-delà de cinq années. Ce délai maximum de conservation vise à obliger

[146] Département du Trésor. « Lettre du département du Trésor des États-Unis concernant SWIFT / programme de surveillance du financement du terrorisme » et « Traitement par le département du Trésor des États-Unis, aux fins de la lutte contre le terrorisme, de données à caractère personnel provenant de l'UE — «SWIFT» ». [En ligne]. Site de l'accès au droit de l'Union européenne. Publication le 20/07/07. Consultation le 08/08/07.
<http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2007/c_166/c_16620070720fr00170017.pdf>
<http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2007/c_166/c_16620070720fr00180025.pdf>
La lettre et les observations sont parues au Journal officiel des Communautés européennes du 20 juillet 2007, respectivement sous les références 2007/C 166/08 et 2007/C 166/09.

l'administration à adopter une gestion rigoureuse des donnés, afin d'éviter que ces données s'accumulent et constituent un stock sans commune mesure avec la finalité du traitement. Il convient de noter que l'engagement américain porte uniquement sur les données inutiles à la lutte contre le terrorisme. Les données qui continueraient à être considérées comme utiles ne sont pas soumises à ce délai maximum de conservation.

- Une « *personnalité européenne éminente* » pourra contrôler le fonctionnement du programme et rendre un rapport annuel sur le respect des engagements du Département du Trésor. Cette garantie consistant dans la présence d'un représentant européen auprès des services du Trésor chargés de l'extraction des données est sans doute le point le plus original de l'engagement américain. Dans un souci de transparence, le gouvernement a en effet accepté la présence d'une « *personnalité européenne éminente* », choisie pour ses compétences en matière de données personnelles, afin de permettre à l'Union européenne de vérifier d'elle-même, directement, le respect de son droit. Cette mesure forte répond directement aux critiques liées au manque de transparence du programme SWIFT et fait de ce programme secret un programme « ouvert ». Il convient en effet de noter que le représentant européen rendra un rapport annuel présentant ses observations sur le fonctionnement du programme au regard des engagements américains. Cette personnalité européenne éminente doit être désignée par la Commission européenne après consultation du président du Comité des représentants permanents (COREPER)[147] et de la Commission des libertés civiles du Parlement européen[148]. Son rapport devra d'abord être présenté à la Commission européenne, qui fera ensuite un rapport au Parlement et au Conseil européen[149]. Les trois principaux organes communautaires seront ainsi à même de contrôler l'application des engagements américains.

L'Union européenne a favorablement accueilli les propositions américaines et a pris note de l'engagement américain de soumettre le programme SWIFT au contrôle d'un représentant européen dans une réponse au Département du Trésor[150]. Une liste est actuellement en cours d'élaboration afin de permettre la désignation d'un représentant qui

---

[147] Le Comité des représentants permanents ou COREPER est chargé de préparer les travaux du Conseil européen. Il est composé des ambassadeurs des États membres auprès de l'Union européenne et est présidé par l'État membre qui assure la Présidence du Conseil.
<http://europa.eu/scadplus/glossary/coreper_fr.htm>

[148] Il convient de noter que la participation du Parlement européen à la désignation de la « personnalité éminente » n'a pas satisfait les eurodéputés, mécontents d'avoir si peu été associés aux négociations après avoir été les seuls à représenter la position européenne du fait de la longue période d'inertie de la Commission et du Conseil européen.
AUTRET, Florence. L'Amérique à Bruxelles. « M. Verheugen, méditez les leçons de SWIFT ». [En ligne]. Publication le 05/07/07. Consultation le 19/07/07.
<http://lobbying.typepad.fr/lamerique_a_bruxelles/2007/07/trouver-le-bon-.html>

[149] Communiqué de presse. « Les États-Unis s'engagent à prendre en compte les principes européens de protection des données pour le traitement des données reçues de Swift ». [En ligne]. Site internet de l'Union européenne. Bruxelles. Publication le 28/06/07. Consultation le 19/07/07.
<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/968&format=HTML&aged=0&language=FR&guiLanguage=en>

[150] Conseil européen et Commission européenne. « Réponse de l'Union européenne au département du Trésor des États-Unis — SWIFT/programme de surveillance du financement du terrorisme ». [En ligne]. Site de l'accès au droit de l'Union européenne. Publication le 20/07/07. Consultation le 08/08/07.
<http://eur-lex.europa.eu/LexUriServ/site/fr/oj/2007/c_166/c_16620070720fr00260026.pdf>
La réponse est parue au Journal officiel des Communautés européennes du 20 juillet 2007 sous la référence 2007/C 166/10.

devrait entrer en fonction « *au cours du premier semestre 2008* ». La personnalité européenne éminente serait « *sans doute un ancien juge* »[151].

La nature juridique de l'engagement américain

Alors que le Parlement européen appelait de ses vœux un véritable accord international, c'est-à-dire un traité, la nature de l'engagement américain est toute autre. Issu d'une concertation entre Union européenne et Etats-Unis, cet engagement consiste en un acte unilatéral du gouvernement américain dont la portée doit être précisée. On parle ici d'échange de lettres et non de traité international. Il ne fait pas de doute que l'engagement américain, exprimé publiquement par le gouvernement américain dans l'intention de se lier, lui impose des obligations[152]. Il s'agit bien d'un engagement juridique lequel, sans être irréversible, ne peut toutefois être remis en cause sans passer par les procédures ordinaires de règlement des différends en droit international public. En tout état de cause, l'application de l'engagement doit se faire dans le respect du principe de bonne foi, principe essentiel du droit des relations internationales. Il ne s'agit donc pas ici d'un simple engagement moral ou *gentlemen's agreement*, dont la force juridique serait bien moindre. De tels actes ne sont en effet pas soumis au droit des traités et sont dépourvus d'effet obligatoire des conventions, la règle *pacta sunt servanda* ne trouvant pas à s'appliquer[153].

L'engagement unilatéral du Département du Trésor, adressé à la Commission et au Conseil européen, engage donc le gouvernement américain.

---

[151] Journal Chrétien. « Swift : les Etats-Unis offrent des garanties ». [En ligne]. Site internet du journal. Publication le 30/06/07. Consultation le 11/07/07.
<http://www.spcm.org/Journal/spip.php?article13001>

[152] Sur ce point, voir DAILLIER, Patrick, NGUYEN QUOC, Dinh et PELLET, Alain. Droit international public. Paris : LGDJ, 1995 (5ème éd.). p.357 et s.

[153] *Ibid.*, p.377 et s.

Chapitre II : Les mesures consenties par le secteur financier en faveur du respect des données personnelles

Si l'administration est à l'origine des violations du droit européen des données personnelles par la société SWIFT, il n'en demeure pas moins que cette dernière, ainsi que nombre d'institutions financières concernées, ont commis des fautes susceptibles d'engager leur responsabilité. Des mesures ont ainsi été recherchées auprès de ces entités qui ont permis, par leur action ou leur abstention, que des atteintes graves soient portées à la protection des données. Nous envisagerons tout d'abord les garanties mises en place par la société belge **(1)** avant d'examiner les efforts consentis par les institutions bancaires **(2)**.

Section I : Les mesures prises par la société SWIFT

L'absence de poursuites judiciaires contre la société SWIFT

Il est rapidement apparu que des sanctions contre la société SWIFT n'auraient pas permis de remédier à ce qui constitue le fond de l'Affaire SWIFT, c'est-à-dire la violation continue des données à caractère personnel requises par le Département du Trésor. En outre, des sanctions à l'encontre de la société n'auraient pas permis de résoudre le conflit de normes à l'origine du litige entre les Etats-Unis et l'Union européenne (*cf infra*). L'enjeu principal de l'Affaire, au regard du droit des données personnelles et de la vie privée, est en effet l'encadrement voire la cessation des transferts de données européennes vers les Etats-Unis. Or c'est bien la société SWIFT qui opère matériellement ces transferts. Elle n'a d'ailleurs pas cessé de livrer ses données après la révélation de l'Affaire[154].

Il convient de noter toutefois qu'aucune poursuite judiciaire contre la société SWIFT n'a abouti. Cette dernière apparaît en effet davantage comme un simple instrument utilisé par le gouvernement américain avant d'être critiqué par les autorités communautaires. Il n'en demeure pas moins que la responsabilité de SWIFT a été reconnue par de nombreuses institutions européennes : la CPVP belge, le Groupe de l'article 29, le Parlement européen, la CNIL… Tout en négociant directement avec le gouvernement américain, les autorités européennes ont donc souhaité obtenir de la société SWIFT elle-même des garanties en termes de protection des données.

La modification de l'architecture du réseau de communication

Les activités de SWIFT consistent dans la fourniture d'une prestation de service de messagerie entre institutions financières. Ce service passe par un réseau physique dont nous avons exposé le fonctionnement en introduction. Les messages traités par SWIFT sont ainsi conservés en double exemplaire, l'un sur un serveur européen, l'autre sur un serveur américain. Le dédoublement des données conservées par SWIFT résulte de la copie systématique des données d'un serveur vers l'autre.

[154] Le Département du Trésor aurait ainsi adressé six *subpoenas* entre juillet 2006 et juin 2007 :
7sur7. « Le Trésor américain continue à se servir de Swift ». [En ligne]. Site internet d'actualités. Publication le 21/06/07. Consultation le 19/07/07.
<http://www.7sur7.be/hlns/cache/det/art_500953.html>

C'est ce mécanisme de copie de sauvegarde (*back-up*) qui permet à l'administration américaine d'accéder secrètement – mais dans le respect du droit américain – à l'ensemble des données conservées par la société. La localisation du serveur a ainsi rendu possible la réquisition des données par le Département du Trésor, tant matériellement que juridiquement. Il a donc été envisagé qu'à l'avenir, ces données soient conservées en un lieu non soumis au droit américain, ce qui priverait d'effet les demandes américaines.

Pour ce faire, une réorganisation de l'architecture du réseau SWIFT elle-même a été envisagée. Cette réorganisation amènerait la société à modifier l'ensemble de la structure physique de son réseau de communication et de conservation des données. Il convient de noter que cette modification a été envisagée par plusieurs acteurs de l'Affaire, dont la société SWIFT elle-même : la mesure a ainsi été préconisée par les membres de son conseil d'administration, qui ont recommandé de « régionaliser » le traitement des données en conservant les données définies comme européennes uniquement en Europe. Ces mesures ont également été appelées de leurs vœux par nombre de banques et d'entreprises clientes de SWIFT[155].

La société SWIFT, qui a négocié à partir de décembre 2006 avec la CPVP belge afin de rendre son activité conforme au droit européen des données personnelles, a ainsi annoncé un plan de réorganisation de l'architecture de son réseau en mars 2007[156]. Un second plan a été annoncé en juin 2007[157]. Ce dernier, explicitement motivé par sa mise en conformité avec le droit européen, doit effectivement permettre à SWIFT de conserver les données « *intra-européennes* » exclusivement en Europe. L'approbation de ce plan par le conseil d'administration est prévue pour la fin du mois de septembre 2007[158].

La question de la détermination des données qui devraient être stockées en Europe reste toutefois sans réponse. En effet, la notion de données « *intra-européennes* » n'est pas une notion juridique et ne permet pas d'établir des critères précis quant aux données concernées. La protection conférée par une architecture renouvelée du réseau demeure donc extrêmement incertaine quant à son étendue.

Le droit européen s'applique à toutes les données personnelles faisant l'objet d'un traitement en Europe, que l'individu concerné soit citoyen de l'Union européenne ou pas. Or la notion même de données « *intra-européennes* » semble plus restrictive que le champ d'application du droit européen. Il est peu probable qu'elle couvrira toutes les données auxquelles s'applique aujourd'hui la Directive 95/56/CE. Des données à caractère personnel, traitées sur le territoire de l'Union européenne et donc régies par son droit, pourraient continuer d'être conservées sur le territoire américain. La réorganisation de l'architecture du réseau n'aurait alors aucune incidence sur la protection conférée à ces données.

Pour ces raisons, il conviendra de suivre attentivement la mise en œuvre technique du chantier de réorganisation du réseau SWIFT, notamment en ce qui concerne le sort des données non considérées comme « *intra-européennes* » mais qui seraient pourtant traitées sur

---

[155] BALLARD Mark. « *Banks want data pulled from US* ». [En ligne]. Site internet *The register*. Publication le 03/07/07. Consultation le 06/08/07.
<http://www.theregister.com/2007/07/03/swift_us_pull/>

[156] SWIFT SCRL. « Actions importantes découlant de la réunion du Conseil d'administration de mars 2007». [En ligne]. Site internet de la société. Publication le 29/03/07. Consultation le 16/06/07.
<http://www.swift.com/index.cfm?item_id=61630>

[157] SWIFT SCRL. « *SWIFT announces plans for system re-architecture* ». [En ligne]. Site internet de la société. Publication le 15/06/07. Consultation le 08/07/07.
<http://www.swift.com/index.cfm?item_id=62260>

[158] SWIFT SCRL. « *SWIFT completes transparency improvements and obtains registration for Safe Harbor* ». [En ligne]. Site internet de la société. Publication le 20/07/07. Consultation le 02/08/07.
<http://www.swift.com/index.cfm?item_id=62669>

le territoire de l'Union. De nouveaux éléments permettront peut-être de répondre à ces questions à partir de la fin du mois de septembre 2007, lors de la présentation du plan de réorganisation au conseil d'administration.

Pour encadrer le transfert de données vers les Etats-Unis, diverses solutions juridiques ont été envisagées indépendamment des évolutions à venir de l'architecture du réseau SWIFT. Ces solutions ont en commun permettre la continuation du transfert de données personnelles vers le serveur américain de SWIFT, mais dans des conditions respectueuses du droit européen des données personnelles. Il convient de remarquer que les garanties envisagées ici répondent aux constats de violation de la Directive 95/46/CE par la CPVP belge puis par le G29 dans leurs avis respectifs (*cf supra*).

L'exécution de l'obligation d'information des personnes concernées[159]

Pour satisfaire à l'obligation d'information posée par la Directive, les clients des banques doivent être informés que leurs données sont susceptibles d'être transférées sur un serveur situé aux Etats-Unis et d'y être requises par les autorités américaines. SWIFT est en effet considéré comme responsable du traitement des données qui transitent sur son réseau, ce qui lui impose de respecter une obligation d'information.

Pour se libérer de l'exécution de cette obligation, la société a invoqué à de multiples reprises l'absence de rapports directs avec les clients des banques. Il lui a été répliqué que sa proximité avec les banques rendait tout à fait possible la transmission des informations aux clients par l'intermédiaire de ces mêmes banques[160]. Il convient de noter que la société semble s'être ralliée à la position de la CPVP sur cette question, en proposant fin mars 2007 d'améliorer la transparence quant au traitement des données de messagerie financière, « *y compris pour les clients des banques* »[161]. En pratique, certaines banques semblent avoir effectivement mis en œuvre ces mesures d'information, la plupart d'entre elles s'étant engagées à informer leurs clients avant septembre 2007[162]. Il faut ici rappeler que les banques sont considérées comme coresponsables des traitements mis en œuvre par SWIFT et que le secteur bancaire fait l'objet de contrôles d'une sévérité particulière de la part de certaines autorités de protection des données personnelles[163]. Cette attention portée aux activités

[159] Article 11 de la Directive 95/46/CE.

[160] SWIFT est une société coopérative, détenue et contrôlée par les plus importantes banques mondiales. Elle compte plus de 2000 adhérents. Elle entretient de ce fait des relations étroites avec le secteur financier, qui est à l'origine de sa création en 1973. Cette proximité et la possibilité de transmettre les informations par l'intermédiaire des banques sont relevées par la CPVP dans son avis du 27 septembre 2006, p.17.
CPVP. « Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC) ». [En ligne]. Site internet de la Commission. Publication le 27/09/06. Consultation le 25/03/07.
<http://www.privacycommission.be/fr/docs/Commission/2006/avis_37_2006.pdf>

[161] SWIFT SCRL. « Actions importantes découlant de la réunion du Conseil d'administration de mars 2007». [En ligne]. Site internet de la société. Publication le 29/03/07. Consultation le 16/06/07.
<http://www.swift.com/index.cfm?item_id=61630>

[162] RAFAL Olivier. « L'UE autorise Swift à transmettre des données personnelles, sous condition ». [En ligne]. Site internet du journal Le Monde informatique. Publication le 29/06/07. Consultation le 25/07/07.
<http://www.lemondeinformatique.fr/actualites/lire-l-ue-autorise-swift-a-transmettre-des-donnees-personnelles-sous-condition-23319.html>

[163] Ainsi que l'a démontré la condamnation pécuniaire du Crédit Lyonnais par la CNIL, le 28 juin 2006.
CNIL. « Délibération n°2006-174 du 28 juin 2006 prononçant une sanction pécuniaire à l'encontre du Crédit Lyonnais (LCL) ». [En ligne]. Site internet de la Commission. Publication le 28/06/07. Consultation le 19/07/07.
<http://www.cnil.fr/fileadmin/documents/approfondir/dossier/banque/D2006_174_Credit_Lyonnais.pdf>

bancaires explique pour partie la célérité des institutions du secteur à prendre en considération les impératifs résultant du droit à la vie privée.

La question demeure toutefois posée de savoir quelle suite serait donnée au refus de certains clients de voir des données transmises aux Etats-Unis, *a fortiori* au Département du Trésor. Les conséquences de ce refus devront être précisées par les banques, notamment quant aux conséquences sur la relation contractuelle entre la banque et son client. Il convient de noter que la réorganisation de l'architecture du réseau que nous avons évoquée permettrait de répondre en partie à un tel refus, puisque cette réorganisation permettrait de conserver exclusivement en Europe les données du client qui refuserait de voir ses données transférées aux Etats-Unis.

La mise en place de « garanties suffisantes » - Les exceptions à l'interdiction des transferts hors Union européenne posée par la Directive

Afin de régulariser les transferts opérés par SWIFT vers les Etats-Unis, une solution a été recherchée au sein de la Directive 95/46/CE elle-même. Si le texte interdit les transferts de données personnelles vers les pays ne présentant pas un niveau de protection adéquat[164], il prévoit des exceptions afin de rendre possible des transferts vers ces pays, à certaines conditions[165].

Nous avons déjà évoqué les trois mécanismes conférant des « garanties suffisantes » au sens de la Directive, qui ont été précisés par la Commission européenne. Ont ainsi été envisagées les règles internes contraignantes (ou *binding corporate rules*), les clauses contractuelles types ainsi que les principes de la sphère de sécurité (ou *Safe Harbor Principles*). La CPVP a implicitement recommandé, dès septembre 2006, que SWIFT adopte des règles d'entreprise contraignantes[166]. Cette proposition de la CPVP avait été reprise implicitement par le Groupe de l'article 29[167].

La société SWIFT a accepté d'adopter le mécanisme des règles d'entreprise contraignantes. Pour déterminer leur contenu, un groupe de travail a été mis en place par SWIFT et dédié à la protection des données. La société a ainsi annoncé en mars 2007 avoir établi un « groupe de travail sur la protection des données », composé de onze experts en matière de protection des données[168]. Ces experts choisis pour leur connaissance du secteur bancaire ont eu pour mission de rechercher « *des solutions contractuelles* » susceptibles de correspondre aux règles d'entreprise contraignantes. Leurs travaux se sont étalés sur trois mois pour être soumis au conseil d'administration de la société en juin 2007. Le 20 juillet, la société annonçait effectivement la mise en place de nouvelles politiques internes en matière de protection de données[169]. Ces nouvelles politiques sont reprises dans trois documents,

---

[164] Article 25 de la Directive.
[165] Article 26 de la Directive.
[166] Avis précité du 27 septembre 2006, p.19.
[167] Groupe de l'article 29. « Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) ». [En ligne]. Site internet de la Commission européenne. Publication le 22/11/06. Consultation le 05/01/07.
<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf>
Voir les « mesures à adopter dans l'immédiat pour redresser la situation actuelle », p.30.
[168] SWIFT SCRL. « Actions importantes découlant de la réunion du Conseil d'administration de mars 2007». [En ligne]. Site internet de la société. Publication le 29/03/07. Consultation le 16/06/07.
<http://www.swift.com/index.cfm?item_id=61630>
[169] SWIFT SCRL. « *SWIFT completes transparency improvements and obtains registration for Safe Harbor* ». [En ligne]. Site internet de la société. Publication le 20/07/07. Consultation le 02/08/07.
<http://www.swift.com/index.cfm?item_id=62669>

disponibles sur le site de la société : elles portent sur l'extraction des données, la protection des données personnelles ainsi que sur l'adhésion aux principes de la sphère de sécurité (*Safe Harbor*). Sans entrer dans le détail de ces différentes règles internes à la société, il convient de noter qu'elles sont susceptibles de régulariser les transferts de données personnelles vers le serveur américain, conformément à l'article 26 de la Directive.

La politique d'extraction des données vise l'usage et la divulgation des données contenues dans les messages. Cette politique interne, qui préexistait à l'Affaire SWIFT, a seulement fait l'objet d'aménagements destinés à améliorer la transparence du système.

La politique de protection des données personnelles fixe les responsabilités de SWIFT et de ses clients en matière de respect des données personnelles. Elle regroupe des textes auparavant épars ainsi que certaines stipulations des conditions générales d'adhésion à la société coopérative. Ce document constitue une « règle contraignante d'entreprise » conforme aux exigences de la Directive.

Il s'agit de préciser ensuite la politique relative aux principes de la sphère de sécurité. La société SWIFT a en effet adopté, dans le même temps que les règles d'entreprise contraignantes, un second mécanisme permettant de passer outre l'interdiction de transférer des données vers un pays ne présentant pas un niveau de protection adéquat. SWIFT a en effet annoncé sa volonté d'adhérer aux principes du *Safe Harbor* en février 2007[170]. Le groupe de travail établi par la société s'est prononcé sur les implications d'une telle adhésion. Soutenue dans ses démarches par le G29, SWIFT a obtenu son enregistrement au titre de ce programme auprès du Département du Commerce américain le 19 juillet 2007[171]. L'adhésion aux principes du *Safe Harbor* garantit que les données stockées dans le centre opérationnel américain sont protégées conformément à des garanties analogues à celles en vigueur en Europe[172].

Depuis l'adhésion au Safe Harbor et la mise en place de règles d'entreprise contraignantes, les transferts de données vers les Etats-Unis sont donc doublement protégés par des garanties que la Commission européenne considère comme « suffisantes » en vertu de la Directive 95/46/CE. Si l'utilité du dédoublement de garanties n'est pas certaine, il a néanmoins pour vertu d'afficher la bonne volonté de SWIFT.

Enfin, il convient de rappeler ici que le troisième mécanisme offert par la Directive ne pouvait être souscrit par la société. En effet, les clauses contractuelles types, posées par la Commission européenne, sont destinées à protéger les transferts intervenant entre deux personnes juridiques distinctes, l'une étant responsable de traitement (ou « exportateur de données »), l'autre étant sous-traitant (ou « importateur de données »). En l'espèce, si SWIFT transfère bien des données vers sa filiale américaine – responsable du serveur accueillant la base de données, le transfert intervient au sein d'une même personne juridique : la société internationale SWIFT. Les clauses contractuelles types n'étaient donc pas applicables.

---

[170] SWIFT SCRL. « *US terrorist financing investigations and the role of SWIFT* ». [En ligne]. Site internet de la société. Publication le 11/02/07. Consultation le 02/06/07.
<http://www.swift.com/index.cfm?item_id=61228>

[171] Département du commerce. Répertoire des organisations ayant adhéré aux principes du *Safe Harbor*, dont SWIFT. [En ligne]. Publication le 19/07/07. Consultation 05/08/07.
<http://web.ita.doc.gov/safeharbor/SHList.nsf/4cd91526e2d0dfa085256967004eb5d7/53a98f15c156d3b08525731d007381f3?OpenDocument>

[172] Pour de plus amples développements sur les principes de la sphère de sécurité :
POULLET Yves. « Les *Safe Harbor Principles* – Une protection adéquate » in *Actes du colloque de l'International Federation of Computer Law Associations (IFCLA) tenu à Paris les 15 et 16 juin 2000*. [En ligne]. Site internet Juriscom. Publication le 17/06/2000. Consultation le 06/05/07.
<http://www.juriscom.net/uni/doc/20000617.htm>

Section II : Les mesures prises par les institutions bancaires

Le rôle des banques clientes de SWIFT

Les autorités européennes n'ont pas manqué de relever la responsabilité des institutions bancaires et financières concernées, à quelque titre que ce soit, par les activités de SWIFT. Des mesures ont ainsi été prises afin de renforcer la transparence et les contrôles quant au respect des données personnelles dans le secteur bancaire et financier.

Dans son avis du 27 septembre 2006, la Commission de la protection de la vie privée belge estimait ainsi que les banques clientes de SWIFT étaient coresponsables du traitement des données de leurs clients échangées sur SWIFTNet Fin[173]. Cette qualité de coresponsable de traitement impose aux banques des obligations comparables à celles de SWIFT. La responsabilité de la Banque nationale de Belgique (BNB), membre du conseil de surveillance de SWIFT, fait l'objet de développements particuliers par la CPVP. La Commission n'exclut pas que la BNB ait pu violer les obligations posées par le droit européen en tant que banque cliente de SWIFT et coresponsable du traitement SWIFTNet Fin. En revanche, elle considère que la BNB, bien qu'informée par SWIFT de l'existence d'une *subpoena* en février 2002, n'a pas violé le droit des données personnelles en tant que membre du conseil de surveillance. Nous verrons en effet que les banques membres du conseil de surveillance ont invoqué leur incompétence en matière de protection des données personnelles, leur mission se limitant dans ce cadre à la stabilité financière (*cf infra*).

L'avis du G29, sur cette question de la responsabilité des banques, rappelle que certaines des banques utilisatrices de SWIFTNet Fin ont été informées de l'existence du programme secret américain. En outre, à compter de la révélation de l'Affaire, toutes les banques sont réputées avoir eu connaissance du programme. Parties prenantes à la société coopérative SWIFT[174], elles sont coresponsables du traitement des données personnelles de leurs clients opéré par SWIFTNet Fin[175] et doivent donc exécuter les obligations imposées par le droit européen.

Le rôle des banques centrales en tant que membres du conseil de surveillance de SWIFT

L'avis rendu par le G29, le 22 novembre 2006, se prononce sur le cas particulier des banques centrales. Les banques centrales du Groupe des Dix[176] participent en effet au conseil de surveillance de SWIFT, notamment les banques nationales belge, allemande, française,

---

[173] Commission de la protection de la vie privée. « Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC) ». [En ligne]. Site internet de la Commission. Publication le 27/09/06. Consultation le 25/03/07. p.13 à 15.
<http://www.privacycommission.be/fr/docs/Commission/2006/avis_37_2006.pdf>

[174] *Cf* note 140.

[175] Groupe de l'article 29. « Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT) ». [En ligne]. Site internet de la Commission européenne. Publication le 22/11/06. Consultation le 05/01/07. p.13 à 15.
<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf>

[176] Le Groupe des Dix se compose de onze pays industriels (Allemagne, Belgique, Canada, Etats-Unis, France, Italie, Japon, Pays-Bas, Royaume-Uni, Suède et Suisse) qui se consultent et coopèrent sur les questions monétaires et financières. Voir la page du Groupe sur le site de l'OCDE :
<http://www.oecd.org/document/24/0,3343,fr_2649_34115_36253592_1_1_1_1,00.html>

italienne, hollandaise, anglaise et suédoise, mais aussi la BCE. Elles ont toutes été informées de la réception par SWIFT des *subpoenas* américaines et de la livraison des données au Département du Trésor[177].

La mission de surveillance vise en premier lieu la stabilité financière et la bonne santé des institutions financières. Le G29 admet donc que les banques centrales membres du conseil de surveillance n'avaient pas à intervenir en cette qualité. Si le conseil de surveillance dispose d'un poids considérable dans la prise de décision au sein de la société SWIFT, la « pression morale » dont il dispose n'avait pas vocation à être exercée pour imposer des pratiques respectueuses du droit des données personnelles.

Le rôle de la Banque centrale européenne (BCE)

Mise en cause par le Parlement européen, la BCE a répondu le 30 janvier 2007 à un courrier du 22 décembre 2006 adressé par les présidents de la commission des libertés civiles et de la commission des affaires économiques[178]. Cette lettre du Président de la BCE, Jean-Pierre Trichet, répond aux questions posées par le Parlement. Elle expose notamment que la BCE, en tant qu'utilisateur de SWIFTNet Fin, ne traitera pas les ordres de paiements émanant de personnes physiques ne donnant pas leur accord à l'utilisation du système SWIFT. Elle se considère incompétente non seulement pour mettre en œuvre des solutions techniques telles que la réorganisation du réseau SWIFT mais encore pour exercer une mission de surveillance sur SWIFT qui comprendrait le contrôle du respect des données personnelles. Elle rappelle à cet égard que sa mission de surveillance se limite à *« la sécurité technique, la fiabilité opérationnelle, la résistance et la bonne gouvernance [de SWIFT]* » ainsi que « *la mise en place de procédures et de contrôle de gestion des risques* »[179]. Elle s'estime enfin incompétente pour contrôler que la société SWIFT ne participe pas à un système d'espionnage économique ou industriel. S'agissant de la question du secret professionnel comme obstacle à la révélation de l'Affaire aux autorités compétentes, la BCE maintient qu'« *elle ne peut accepter que ses obligations de confidentialité ne soient pas respectées* ».

Cette réponse à la question du Parlement européen, qui l'interrogeait sur l'opportunité d'invoquer le secret professionnel dans l'hypothèse d'une « *violation éventuelle des droits constitutionnels ou des droits de l'homme* », ne manque pas de surprendre. En effet, cette conception extensive du secret professionnel a pour conséquence une neutralité bancaire qui pourrait confiner à des abstentions coupables. Comment admettre que la banque centrale de l'Union européenne se réfugie derrière le secret professionnel, qui n'a qu'une valeur légale, pour refuser de dénoncer les violations de droits aussi éminents que ceux protégés par des textes tels que la CESDH ou encore les constitutions des Etats membres ?

---

[177] La Banque nationale de Belgique, ainsi que la BCE, aurait été informées de l'accès aux données de SWIFT par l'administration américaine dès février 2002. Les autres banques du Groupe des Dix l'auraient appris quatre mois plus tard.
STROOBANTS, Jean-Pierre. « Espionnage bancaire par la CIA : la Banque de Belgique était au courant depuis 2002 ». [En ligne]. Site du journal Le Monde. Publication le 30/06/06. Consultation le 18/03/07.
<http://www.lemonde.fr/cgi-bin/ACHATS/acheter.cgi?offre=ARCHIVES&type_item=ART_ARCH_30J&objet_id=950954&clef=ARC-TRK-D_01>

[178] Banque centrale européenne. « Lettre du Président de la BCE à M. Jean-Marie Cavada, Président de la commission des libertés civiles, de la justice et des affaires intérieures » et « Lettre du Président de la BCE à Mme Pervenche Berès, Présidente de la Commission des affaires économiques et monétaires ». [En ligne]. Site internet de la BCE. Publication le 30/01/07. Consultation le 18/05/07.
<http://www.ecb.int/pub/pdf/other/070130cavadaswiftfr.pdf>
<http://www.ecb.int/pub/pdf/other/070130beresswiftfr.pdf>

[179] *Ibid.*

La responsabilité de la Banque centrale européenne a fait l'objet d'une enquête approfondie du Contrôleur européen de la protection des données (CEPD), compétent en matière de violation de la protection des donnés personnelles par les organes communautaires. Le CEPD a recommandé que la BCE ainsi que l'ensemble de la communauté financière, « *fournissent des systèmes de paiement qui n'enfreignent pas la réglementation européenne en matière de protection des données* »[180]. Les conclusions de son avis du 1er février 2007 recommandent à la BCE d'agir dans trois directions, qui correspondent à aux trois rôles joués par la Banque centrale dans l'Affaire SWIFT.

Le Contrôleur distinguait 3 rôles de la BCE : la Banque centrale est en effet à la fois chargée de contrôler l'activité de société SWIFT en tant que membre de son conseil de surveillance, en tant que coresponsable du traitement opéré par le service SWIFTNet Fin et en tant que banque centrale c'est-à-dire de « décideur ».

L'avis a ainsi recommandé que la BCE, membre du conseil de surveillance de la société, clarifie les règles de confidentialité ainsi que la gouvernance de SWIFT afin d'assurer que les violations éventuelles de la protection des données personnelles puissent être connues des autorités compétentes en temps utiles. Il est en effet considéré que la BCE, en s'abstenant de révéler le transfert des données aux Etats-Unis, a entretenu le secret d'une action illégale au regard du droit européen. La mission de la BCE se limite toutefois à la protection de la stabilité financière et la ligne de défense de la Banque repose principalement sur son incompétence en matière de protection des données personnelles[181].

Le CEPD a également considéré que la BCE, en tant qu'utilisateur du service SWIFTNet FIN, est coresponsable des traitements mis en œuvre par la société coopérative. Dès lors, elle doit rechercher des solutions permettant de garantir que les transferts de données bancaires de ses clients sont conformes à la réglementation européenne sur la protection des données. Le Contrôleur a donc exigé que la BCE lui remette un rapport sur ces solutions, en se réservant la possibilité d'engager une action contre la banque centrale en application de l'article 47 du règlement 45/2001[182] si elle s'abstenait de présenter ce rapport.

Enfin, en tant que décideur, la BCE doit veiller à ce que l'architecture du système SWIFT ne permette pas de rendre les données traitées accessible de manière routinière, massive et sans garanties à des Etats tiers à l'Union européenne.

---

[180] Contrôleur européen de la protection des données. « Le CEPD demande à la BCE de s'assurer que les systèmes européens de paiement respectent la protection des données ». [En ligne]. Site internet du Contrôleur. Publication le 01/02/07. Consultation le 18/06/07.
<http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2007/EDPS-2007-1-FR_SWIFT.pdf>
L'avis intégral du CEPD sur le rôle de la BCE dans l'Affaire SWIFT est disponible en anglais à l'adresse suivante :
<http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Inquiries/2007/07-02-01_Opinion_ECB_role_SWIFT_EN.pdf>

[181] A ce propos, voir le communiqué de presse faisant suite au discours du Président de la BCE, Jean-Pierre TRICHET, dès le 4 octobre 2006, lors de l'audition publique organisée sur l'Affaire SWIFT par le Parlement européen.
Banque centrale européenne. « *Statement by the President of the ECB at the public hearing at the European Parliament on the interception of bank transfer data from the SWIFT system by the US secret services* ». [En ligne]. Site internet de la BCE. Publication le 04/10/06. Consultation le 12/03/07.
<http://www.ecb.int/press/key/date/2006/html/sp061004.en.html>

[182] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Disponible en ligne.
<http://europa.eu.int/eur-lex/pri/fr/oj/dat/2001/l_008/l_00820010112fr00010022.pdf>

La BCE a publié, le jour même de la publication de l'avis du CEPD, un communiqué de presse répondant aux conclusions de ce dernier[183]. Ce communiqué rappelle l'incompétence de la BCE en matière de protection des données personnelles. La BCE y appelle de ses vœux une évolution du droit applicable lorsque la protection des données personnelles se trouve en conflit avec la lutte contre le terrorisme. La BCE s'engage toutefois à recueillir le consentement de ses cocontractants lors de l'usage des services de SWIFT, conformément au règlement 45/2001 qui protège les données personnelles traitées par les institutions communautaires. On peut noter que ce communiqué de presse reprend les principaux éléments de réponse transmis la veille, par courrier, aux présidents des commissions permanentes des libertés civiles et des affaires économiques, du Parlement européen.

Dans un communiqué ultérieur, en réponse à la résolution du Parlement européen sur l'Affaire SWIFT[184], la BCE a réitéré ses arguments opposés aux présidents des commissions précitées et au CEPD[185].

Au regard des éléments avancés par les différentes institutions financières concernées par l'Affaire SWIFT, il semble que les principaux progrès en matière de protection des données personnelles aient été réalisés par la société SWIFT elle-même. Les banques clientes de SWIFTNet Fin, si elles se sont engagées à mettre en œuvre des mesures d'information à destination de leurs clients, ne semblent pas à même de protéger davantage les données personnelles de leurs clients. En effet, la position de SWIFT sur le marché de la messagerie interbancaire ne permet pas aux banques clientes du service SWIFTNet Fin d'envisager l'utilisation d'un service concurrent, plus respectueux des données personnelles. S'agissant des banques centrales, celles-ci se sont généralement engagées à agir en tant que banques clientes de SWIFT, en arguant de leur incompétence pour rejeter par principe toute mesure supplémentaire.

---

[183] Banque centrale européenne. « *Remarks by the European Central bank on the oversight of SWIFT* ». [En ligne]. Site internet de la BCE. Publication le 01/02/06. Consultation le 27/04/07. <http://www.ecb.int/press/pr/date/2007/html/pr070201.en.html>

[184] Parlement européen. « Résolution du Parlement européen sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions ». [En ligne]. Site internet du Parlement. Publication le 14/02/07. Mise à jour le 01/08/07. Consultation le 06/08/07. <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0039&language=FR&ring=B6-2007-0042>

[185] Banque centrale européenne. « *Remarks by the European Central bank on a resolution passed by the European Parliament relating to the operations of SWIFT* ». [En ligne]. Site internet de la BCE. Publication le 15/02/06. Consultation le 27/04/07. <http://www.ecb.int/press/pr/date/2007/html/pr070215.en.html>

Conclusion

Force est de constater que la résolution de l'Affaire SWIFT intervient au moment où les relations entre l'Union européenne et les Etats-Unis marquent une nette amélioration. Cet apaisement a sans doute joué dans la résolution politique du conflit. Il convient de noter à cet égard que la solution a été négociée assez rapidement et a suscité moins de difficultés que la résolution du dossier PNR.

Toutefois, comme dans d'autres dossiers, les négociations n'ont pas eu pour effet d'entraîner un changement d'attitude radical des Etats-Unis. Si ces derniers ont adopté des comportements plus respectueux des libertés sous la pression des autorités européennes, ils n'ont pas été jusqu'à mettre un terme à leurs projets. L'action européenne ne doit pas être négligée. Elle permet d'amener l'administration américaine à revoir sa position en de nombreuses hypothèses mais aussi à l'Union européenne de réaffirmer progressivement sa souveraineté face à des Etats-Unis omniprésent depuis le 11-Septembre.

L'Affaire SWIFT en est un exemple éclairant. Le droit européen des données personnelles, hautement protecteur, est limité territorialement. La négociation avec le gouvernement américain a toutefois permis d'amener ce dernier à accepter des garanties allant bien au-delà de ce que prévoit le droit des Etats-Unis. Le droit européen tend ainsi à protéger les données où qu'elles soient transmises, par extension. Les principes du *Safe Harbor* mais aussi les garanties exceptionnelles posées par l'engagement unilatéral américain marquent la pénétration des préoccupations européennes hors d'Europe.

Il n'en demeure pas moins que la position européenne n'a pas été dépourvue d'ambigüité. A cet égard, la coopération toute relative de la BCE ainsi que les réticences du Conseil de l'Union à affirmer la souveraineté européenne marquent une certaine faiblesse des organes communautaires. La violation du droit européen, largement imputée à SWIFT, a également pu être reprochée à la Banque centrale européenne, organe communautaire.

S'agissant de la société SWIFT, instrumentalisée par l'administration américain, il convient de rappeler que sa création et son fonctionnement sont marqués par sa proximité avec le secteur financier. Le silence des institutions financières est donc assez naturel au vu de son rôle au sein même de SWIFT. Il revient donc à l'Union européenne d'améliorer l'indépendance de ses institutions financières et bancaires, dont la BCE, face aux Etats-Unis.

Toutefois, la combinaison des mesures résultant de l'Affaire SWIFT, qu'elles soient dirigées vers l'administration américaine ou vers le secteur financier, permettent de considérer aujourd'hui que le transfert de données bancaires vers le Département du Trésor se fait dans des conditions plus respectueuses du droit européen des données personnelles. La conscience de la nécessité de protéger les données personnelles et la vie privée s'en trouve renforcée, non seulement parmi les « pays ne disposant pas d'un niveau de protection adéquat » mais encore dans le secteur financier, qui prend peu à peu conscience de son rôle dans la protection des données qu'il véhicule.

Bibliographie et webographie

Ouvrages – Thèses – Monographies

DAILLIER Patrick, NGUYEN QUOC Dinh et PELLET Alain, *Droit international public*, Paris, LGDJ, 1995 (5ème éd.), 1317 p.

FRANCOIS Ludovic, CHAIGNEAU Pascal et CHESNAY Marc. *Blanchiment et financement du terrorisme*, Paris, Editions Ellipses, 2004, 144 p.

SCHRADER Jeremy S. « *Secrets Hurt: How SWIFT Shook Up Congress, the European Union, and the U.S. Banking Industry* », Mémoire universitaire, Institut bancaire de l'Université de Caroline du Nord, 2007, 24 p.
Publié sur le site de l'Institut :
http://www.unc.edu/ncbank/Articles%20and%20Notes%20PDFs/Volume%2011/Shrader(397-420).pdf

VAISSE Justin et HASSNER Pierre, *Washington et le monde : dilemmes d'une superpuissance*, Paris, Editions Autrement, 2003, 200 p.

Articles de doctrine

ACKERMAN Bruce, « Les pouvoirs d'exception à l'âge du terrorisme » in *Esprit*, août/septembre 2006, 15 p.

BIGNAMI Francesca, « *The U.S. Privacy Act in comparative perspective* » in *Colloque sur PNR/SWIFT/Safe Harbour – Les données transatlantiques sont-elles protégées ? tenu à Bruxelles le 26 mars 2007,* 10 p.
Publié sur le site du Parlement européen :
<http://www.europarl.europa.eu/hearings/20070326/libe/bignami_en.pdf>.

CAPRIOLI Eric A., « Violation des règles propres aux données à caractère personnel et réseau SWIFT », in *Revue de droit bancaire et financier*, janvier-février 2007, 3 p.

HUSTINX Peter, « Vie privée et données personnelles : vers un 'style européen de la société de l'information' » in *Les dossiers européens*, février 2007, 2 p.

LAVENUE Jean-Jacques, « Interopérabilité internationale, interconnexion des fichiers et protection des libertés : interrogation sur le devenir des données transférées dans le cadre de la lutte contre le terrorisme » in *Actes du 1er colloque sur le droit de l'administration électronique tenu à Paris les 6 et 7 décembre 2006*, 22 p.
Publié sur le site du colloque :
http://dae2006.univ-paris1.fr/index.php?option=com_content&task=view&id=116&Itemid=50

RODOTA Stefano, « *The European constitutional model for data protection* », in *Colloque PNR/SWIFT/Safe Harbour – Les données transatlantiques sont-elles protégées ? tenu à Bruxelles le 26 mars 2007*, 4 p.
Publié sur le site du Parlement européen :
<http://www.europarl.europa.eu/hearings/20070326/libe/rodota_en.pdf>

POULLET Yves, « Les *Safe Harbor Principles* – Une protection adéquate » in *Actes du colloque de l'International Federation of Computer Law Associations (IFCLA) tenu à Paris les 15 et 16 juin 2000.*
Publié sur le site Juriscom : http://www.juriscom.net/uni/doc/20000617.htm

POULLET Yves et DEGRAVE Elise, « L'Affaire SWIFT » in *Revue du Droit des Technologies de l'Information* n° 27, 2007, 7 p.

SERVIDIO-DELABRE Eileen, « Chronique de droit américain » in *Revue internationale de droit pénal* vol.72, 2001, 14 p.

Sites internet

Le site d'accès au droit de l'Union européenne
http://eur-lex.europa.eu/
EUR-Lex offre un accès au droit de l'Union européenne. Le système permet de consulter le Journal officiel de l'Union européenne et inclut notamment les traités, la législation, la jurisprudence et les actes préparatoires de la législation. On y trouve les textes juridiques constituant le droit européen de la protection des données à caractère personnel.

Banque centrale européenne
http://www.ecb.int/
Le site de la Banque centrale européenne offre des informations relatives aux activités de l'institution, notamment en matière de politique monétaire et de réglementation des marchés. Une rubrique « Communiqués de presse » permet à la Banque centrale de publier des informations sur ses activités, dont les éléments de réponse à sa mise en cause dans l'Affaire SWIFT.

Commission de la protection de la vie privée
http://www.privacycommission.be/fr/
Le site de la Commission belge permet de disposer des décisions et avis rendus à propos de la protection des données à caractère personnel. Il comporte des guides destinés à l'information des justiciables ainsi qu'une rubrique « Presse ». On y trouve le rapport de la Commission sur le transfert de données bancaires opéré vers les Etats-Unis.

Commission nationale de l'informatique et des libertés
http://www.cnil.fr/
Le site de la Commission française comporte, comme celui de son homologue belge, des documents rendant compte de son activité. Il comprend les rapports annuels de la Commission et une rubrique « Actualité ». Divers communiqués de presse rendent compte de son action dans le suivi de l'Affaire SWIFT.

Commission européenne

http://ec.europa.eu/
Le site de la Commission offre principalement à ses visiteurs des communiqués de presse, des liens vers les politiques gérées et exécutées par la Commission et des liens directs vers ses principaux services d'information. Il permet de prendre connaissance de l'action de la Commission, dont celle du Groupe de l'article 29, à propos de l'Affaire SWIFT.

Conseil de l'Union européenne
http://www.consilium.europa.eu/
Le site du Conseil propose des comptes-rendus sur les politiques menées par l'organe communautaire, une revue de presse et des informations institutionnelles. Il rapporte les positions prises par le Conseil sur l'Affaire SWIFT.

Contrôleur européen de la protection des données
http://www.edps.europa.eu/
Le site du Contrôleur rend compte de ses activités de surveillance et de contrôle quant au respect des données à caractère personnel par les organes communautaires. On y trouve ainsi des informations relatives au contrôle sur la Banque centrale européenne.

Département du Trésor américain
http://www.treas.gov/
Le site du Département du Trésor comprend notamment une rubrique sur la lute contre le financement illicite ainsi qu'une rubrique internationale. Ses archives permettent d'accéder aux réactions de l'administration américaine suite à la révélation de l'Affaire SWIFT.

Groupe de l'article 29
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm
Le site du Groupe, hébergé par la Commission européenne, présente l'organisation, les missions et les documents résultant de l'activité du Groupe sur la protection des données.

Parlement européen
http://www.europarl.europa.eu/
Le site du Parlement reflète l'implication de l'institution dans la protection des libertés. Il contient les résolutions adoptées mais aussi les rapports et les actes de conférences organisées par les eurodéputés autour de l'Affaire SWIFT.

Présidence des Etats-Unis
http://www.whitehouse.gov/
Le site de la Présidence des Etats-Unis comporte différentes rubriques d'actualité ainsi que des archives qui permettent d'accéder aux communiqués présidentiels suite à la révélation de l'Affaire.

Société SWIFT
http://www.swift.com/
Le site de la société présente ses différents services mais également les documents relatifs aux conditions générales de ces services. On y trouve ainsi la politique de SWIFT en matière de protection des données à caractère personnel, mais également les communiqués de presse qui traduisent la réaction de la société au fur et à mesure du déroulement de l'Affaire.

Liste des abbréviations

ACLU : *American Civil Liberties Union* ou « Association américaine pour les libertés civiles »

BCE : Banque centrale européenne

BNB : Banque nationale de Belgique

CEPD : Contrôleur européen de la protection des données

CESDH : Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

CIA : *Central Intelligence Agency* ou « Agence centrale de renseignement »

CJCE : Cour de justice des Communautés européennes

CNIL : Commission nationale de l'informatique et des libertés (France)

CPVP : Commission de la protection de la vie privée (Belgique)

FBI : *Federal Bureau of Investigation* ou « Bureau federal d'investigation »

G29 : Groupe de l'article 29

IEEPA : *International Emergency Economic Powers Act* ou « Loi sur les pouvoirs économiques en cas d'urgence internationale »

LVP : Loi belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

NSA : *National Security Agency* ou « Agence de sécurité nationale »

OFAC : *Office of Foreign Assets Control* ou « Bureau de surveillance des capitaux étrangers »

PNR : *Passenger name record* ou « Données passager »

RFPA : *Right to Financial Privacy Act* ou « Loi sur le droit à la vie privée en matière financière »

TFTP : *Terrorist Finance Tracking Program* ou « Programme de pistage du financement terroriste »

UNPA : *United Nations Participation Act* ou « Loi sur la participation à l'organisation des Nations Unies »

USA PATRIOT ACT : *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* ou « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme »

UST : *United States Treasury* ou « Département du Trésor »

Table des matières