# Europe et privacy : le cas SWIFT : analyse de l'applicabilité de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données

Louveaux, Sophie; Havelange, Benedicte; Poullet, Yves

*Publication date:*
1997

*Document Version*
le PDF de l'éditeur

CENTRE DE RECHERCHES
INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES
NOTRE-DAME DE LA PAIX

# EUROPE ET "PRIVACY": LE CAS SWIFT

## ANALYSE DE L'APPLICABILITE DE LA DIRECTIVE 95/46/CE DU 24 OCTOBRE 1995 RELATIVE A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES

ETUDE REALISEE PAR
SOPHIE LOUVEAUX

Avec la collaboration de BENEDICTE HAVELANGE

sous la direction d'YVES POULLET

AVRIL 1997

# Table des matières


Introduction ..... 1
PARTIE I : GÉNÉRALITÉS CONCERNANT LA DIRECTIVE ..... 1
Chapitre I : Définitions et Champ d'Application ..... 2
Section 1 : Le champ d'application territoriale ..... 2
Section 2 : Les données à caractère personnel ..... 3
Section 3 : Le traitement ..... 4
Section 4 : Le fichier ..... 5
Section 5 : Le responsable du traitement ..... 6
Section 6 : Le sous-traitant ..... 7
Chapitre III : Communication des données ..... 8
Chapitre IV : Flux transfrontières de données ..... 8
Section 1 : Règle générale (article 25) ..... 9
Section 2. Les dérogations (Article 26) ..... 11
2.A. Dérogations spécifiques ..... 11
2.B. Les "clauses contractuelles appropriées" ..... 12
Chapitre V : Application des principes régissant la directive ..... 13
Section 1 : Le principe de finalité ..... 14
1.A. Principe de finalité légitime ..... 14
1.B. Principes relatifs à la légitimation des traitements de données ..... 15
Section 2 : Principes régissant les catégories particulières de données ..... 16
Section 3 : Principes relatifs à la qualité des données ..... 17
Chapitre VI : Obligations du responsable du traitement ..... 17
Section 1 : Obligation d'information (articles 10 et 11) ..... 17
Section 2 : Confidentialité et sécurité des traitements ..... 18
Section 3 : Respect des droits de la personne concernée ..... 19
3.A. Droit d'accès (Article 12) ..... 19
3.B. Droit de rectification (article 12.2.et 12.3) ..... 19
3.C. Droit d'opposition (article 14) ..... 19
3.D. Le droit de ne pas être soumis à une décision individuelle automatisée (article 15) ..... 19
Section IV. Notification à l'autorité de contrôle ..... 20

PARTIE II : APPLICATION A S.W.I.F.T. ..... 21
Chapitre I : Les données contenues dans les messages ..... 21
Section 1 : Définitions ..... 21
1.A. Données à caractère personnel ..... 21
1.B. Traitement ..... 21
1.C. Responsable du traitement ..... 22
1.D. Sous-traitant ..... 24
Chapitre II : Les données générées par l'utilisation du réseau S.W.I.F.T. ..... 25
Section I : La proposition de Directive "télécoms" ..... 26
Section 2 : Application de la directive générale ..... 27
PARTIE III AUTRES SERVICES ..... 28
Chapitre I : Le Service FIN Copy ..... 28
Section 1 : Description du service ..... 28
Section 2 : Application de la directive ..... 29
Chapitre II : Message Retrieval Policy ..... 30
Section 1 : Description du service ..... 30
Section 2 : Application de la directive ..... 30
1.A. Retrait à des fins propres ..... 31
1.B. Retrait pour des finalités définies par le requérant ..... 31
Chapter III : Les conséquences de la qualification de S.W.I.F.T. comme responsable du traitement ..... 32
Conclusion ..... 35

# Introduction

Après de nombreuses propositions et amendements, la directive 95/46/CE du Parlement européen et du Conseil relative a la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, a été adoptée le 24 octobre 1995[1]. En vertu de son article 32, les États membres sont tenus de mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive et ceci avant le 24 octobre 1998. Ce texte pourrait dès lors avoir des implications significatives sur les activités menées par S.W.I.F.T. dans la mesure où celles-ci peuvent concerner des données à caractère personnel, objet de la protection envisagée.

Dans une première partie de cette étude, les concepts de base de la directive et les principes régissant cette dernière seront étudiés dans une perspective assez théorique. L'objectif de cette partie est avant tout de poser le cadre d'analyse à l'étude entreprise.

Dans une deuxième partie, nous tenterons d'appliquer la directive aux service de messagerie offert par le réseau S.W.I.F.T. (FIN Service). Nous distinguons à cet égard entre l'application aux données contenues dans le message lui-même (message data) et les données générées par l'utilisation du réseau (traffic data).

Enfin, dans une troisième partie, nous centrerons notre analyse sur l'application de la directive aux deux nouveaux services développés par S.W.I.F.T. que sont FIN Copy et Message Retrieval.

# Partie I : Généralités concernant la Directive

Il ne s'agit pas ici de passer en revue l'ensemble des dispositions contenues dans la directive mais de définir selon les termes mêmes du texte de cette dernière et d'analyser les notions indispensables pour résoudre la question de son application au réseau S.W.I.F.T. D'autre part, une analyse du texte de la proposition de directive[2] ayant déjà été menée[3], nous nous contenterons d'analyser les notions qui ont subi des

[1] Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O., 23.11.95, n° L 281/31. Ci-après: "directive".

2 Proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel, document COM (90) 314 final SYN 287 (13 septembre 1990). Ci-après: "proposition de directive".

[3] "EUROPE ET "PRIVACY": LE CAS SWIFT, Analyse de la proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel",

modifications dans la version définitive de la directive telle que nous la connaissons aujourd'hui.

## CHAPITRE I : DÉFINITIONS ET CHAMP D'APPLICATION

Afin de mesurer l'impact de la directive sur le réseau S.W.I.F.T., il est nécessaire de cerner avec précision le champ d'application territoriale visé ainsi que l'objet de la protection envisagée. A cette fin nous procéderons dans une première section à l'analyse de l'article 4 de la directive ("Droit national applicable"). Ensuite nous examinerons les notions définies dans le texte qui nous paraissent les plus pertinentes dans l'étude de l'application de la directive au réseau S.W.I.F.T. en ne soulignant que les modifications par rapport à la version initiale de proposition de directive : données à caractère personnel (section 2), le traitement (section 3), le fichier (section 4), le responsable du fichier (section 5), le sous-traitant (section 6).

### *Section 1 : Le champ d'application territoriale*

La proposition de directive initiale, retenait le lieu de localisation du fichier afin de déterminer la loi nationale applicable[4]. Ce critère n'a plus été retenu, la localisation d'un fichier ou d'un traitement étant souvent difficile voire même impossible à déterminer : dans un contexte de réseau, les fichiers pourront être répartis dans plusieurs États membres sans que l'on puisse en définir la localisation exacte.

Selon la directive actuelle, c'est l'établissement[5] du responsable du traitement sur le territoire d'un État membre qui détermine le droit national applicable. En effet, d'après l'article 4 de la directive, chaque État membre applique les dispositions nationales prises en vertu de la directive aux traitement de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités d'un établissement de

---

Étude réalisée par Marie-Hélène BOULANGER et Thierry LEONARD sous la direction de YVES POULLET, Centre de recherche Informatique et Droit, Juin 1992.

[4] Par "fichier" au sens de la proposition de directive, il faut entendre "tout ensemble de données à caractère personnel, centralisées ou réparties sur plusieurs sites, faisant l'objet d'un traitement automatisé ou qui, bien que ne le faisant pas, sont structurées et accessibles dans une collection organisée selon des critères déterminés de manière à faciliter l'utilisation ou l'interconnexion des données" (article 2.c.). La proposition de directive prévoyait que la législation d'un État membre contenant la transposition des principes de la directive s'appliquait : 1°) à tous les fichiers localisées sur son territoire; 2°) au responsable du fichier qui réside sur ce territoire et utilise depuis un fichier localisé dans un pays tiers dont la législation n'a pas un niveau de protection adéquat, à moins que l'utilisation ne soit sporadique.

[5] Selon le considérant 19 de la directive, l'établissement dans un État membre suppose "l'exercice réel et effectif d'une activité au moyen d'une installation stable". La forme juridique retenue par l'établissement (filiale, succursale,...) est sans influence à cet égard.

responsable du traitement sur le territoire d'un État membre. Si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable [6].

Lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté mais qu'il recourt, à des fins de traitement de données à caractère personnel à des moyens, automatisés ou non, situés sur le territoire d'un État membre, la législation nationale de cet État s'applique, sauf si les moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté. Le responsable du traitement sera tenu de nommer un représentant établi sur le territoire dudit État membre[7]. La nomination de ce représentant s'opère sans préjudice des actions qui pourraient être intentées contre le responsable lui-même[8]. Il n'est cependant pas facile de déterminer ce que l'on entend par "recourt à des moyens". La simple consultation d'une base de données située sur le territoire d'un État membre par un individu se trouvant dans un pays hors de l'Union, implique-t-elle le respect de la législation nationale en vigueur et la nomination d'un représentant? De même, le terme de "transit" n'est guère plus explicite. Est-il lié à une notion de durée du traitement ou de manque d'enregistrement des données ?

## ***Section 2 : Les données à caractère personnel***

Afin de circonscrire le champ d'application de la directive, il faut préciser la notion de "données à caractère personnel".

La définition retenue est quasi identique à celle retenue par la proposition initiale à savoir "toute information concernant une personne physique identifiée ou identifiable"[9]. Le texte va cependant plus loin dans l'explicitation de ce que l'on entend par "personne identifiable" : "une 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". Le concept retenu est dès lors assez large et peut recouvrir une large gamme de données telles qu'un numéro de compte en banque, une photo, un numéro de client,....

L'identification peut se faire directement (par un nom) ou indirectement, sur base d'une seule donnée (numéro de passeport, de sécurité sociale,...) ou sur base d'un

---

6 Directive, article 4.a.

7 Directive, article 4.1.c. et 4.2.

8 Il s'agit en réalité de nommer un interlocuteur proche de la personne concernée qui pourra plus facilement remplir certaines des obligations prévues à charge du responsable (obligation d'information, obligation de notification auprès de l'autorité de contrôle,...).

9 Directive, article 2.a.

ensemble de données a priori inoffensives mais qui, prises ensembles, permettent d'identifier la personne concernée (age, domicile, sexe, numéro de téléphone...). La définition permet également de retenir des données telles que la voix, l'image, les empreintes génétiques,... Sont considérées comme des données à caractère personnel, uniquement les données qui sont relatives à une personne physique. Les personnes morales et les groupements sont donc exclus de la protection mise en place par la directive générale[10]. Toutefois si les données relatives à une personne physique (les noms des administrateurs d'une société ou des membres d'une association sans but lucratif) sont intégrées parmi des données relatives à des personnes morales, elles bénéficieront de la protection de la directive.

La notion d'"anonymisation" n'a pas été retenu par la version finale directive[11], la référence à un effort excessif étant trop relative et dépendante des moyens dont dispose le détenteur des moyens[12].

## ***Section 3 : Le traitement***

Contrairement à la proposition de directive initiale, ce n'est plus la notion de "fichier" qui est au centre de la protection mise en place par la directive[13]. Si ce critère était pertinent d'un point de vue formel, dans la mesure où il offrait une base matérielle pour les formalités administratives (notification de l'autorité de contrôle, information de la personne concernée,...), comme nous l'avons déjà précisé, il a vite été jugé dépassé dans un contexte de réseaux où il est difficile de localiser un "fichier". La directive a donc adopté un concept beaucoup plus large, tenant compte de l'évolution de la technologie.

C'est l'existence ou non d'un "traitement" qui conditionne l'applicabilité de la directive : "la directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à être contenues dans un fichier"[14] .

Par "traitement" il faut entendre "toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la

---

[10] Il n'en est pas de même pour la directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, en particulier des réseaux numériques à intégration de services (RNIS) et des réseaux mobiles numériques publics (96/C 315/06). Pour l'analyse de ce texte, voir *infra*.

[11] Au sens de la proposition de directive, la donnée anonyme est celle qui ne peut plus être reliée à une personne physique déterminée ou déterminable, "ou moyennant seulement un effort excessif en personnel, en frais et en temps". Article 2.b. de la proposition initiale de directive.

[12] Voir à ce propos commentaires par M-H. BOULANGER et TH. LEONARD dans étude précédente, page 7.

[13] Selon la directive, la notion de fichier sert actuellement à identifier les traitements non automatisés tombant dans le champ d'application de la directive (cfr. *infra* section 5).

[14] Directive, article 3.1.

conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction"[15]. Ces opérations mentionnées dans l'article 2 de la directive ne le sont qu'à titre d'exemples. De sorte que l'on peut dire qu'à partir du moment où les données sont collectées, toute utilisation de celles-ci, en ce compris la collecte elle-même, fait partie intégrante du traitement. La notion de traitement est donc très étendue.

Le traitement, au sens donné par la directive, peut être constitué par une opération poursuivant à elle seule une finalité déterminée (communication des données à des fins de marketing), ou par un ensemble d'opérations. Dans ce cas le critère d'unité entre les différentes opérations est à rechercher dans la finalité poursuivie par celui qui met en oeuvre le traitement. En effet, le traitement des données poursuit toujours un but déterminé, les opérations effectuées sur les données s'apprécieront en fonction de celui-ci.

Le critère de la finalité comme fondement de la détermination d'un traitement répond d'ailleurs à la logique de la protection mise en place par la directive. La protection offerte par la directive est, en effet, centrée sur la notion de traitement. C'est la finalité qui détermine la légitimité du traitement (article 6). Une fois cette finalité déclarée, les données ne peuvent plus être utilisées pour d'autres buts incompatibles. C'est encore en fonction de la finalité que l'on peut contrôler la qualité des données : celles-ci doivent être adéquates, pertinentes et non excessives par rapport à la finalité poursuivie. La durée de conservation des données s'apprécie également en fonction de la finalité du traitement.

## ***Section 4 : Le fichier***

Le terme de fichier reste utile afin de déterminer les traitements non automatisés tombant dans le champ d'application de la directive : seuls les traitements non automatisés de données à caractère personnel qui sont contenues ou appelées à figurer dans un fichier, sont couvertes. Par "fichier", il faut entendre "tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé ou décentralisé ou reparti de manière fonctionnelle ou géographique"[16].

La décentralisation fonctionnelle ou géographique est donc sans importance. Ce qui compte c'est l'accessibilité des données, c'est que ces données soient structurées

---

[15] Directive, article 2.b.
[16] Directive, article 2.c.

selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel[17]. Ainsi par exemple, un ensemble de fiches classées par un concessionnaire en voitures d'occasion, en fonction de la marque de la voiture ne sera pas considéré comme un fichier de données à caractère personnel, même si les noms de l'acheteur et du vendeur sont repris sur ces fiches. Les données à caractère personnel qui ne sont pas organisés en vue de leur usage vis-à-vis des personnes concernées, ne présentent pas les mêmes risques et il n'est dès lors pas réaliste de les soumettre aux mêmes obligations[18].

## ***Section 5 : Le responsable du traitement***

La notion de responsable du fichier a été abandonné au profit de la notion de "responsable du traitement". Il s'agit, selon l'article 2.d. de la directive, "de 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"[19]. Le responsable du traitement est donc la personne qui décide en dernier ressort, seul ou conjointement, de la finalité et des moyens[20] du traitement.

Afin de faciliter la reconnaissance de droits dans le chef des personnes concernées, c'est au responsable du traitement, ou à son représentant[21] qu'incombe le respect de la plupart des obligations prévues par la directive. Ainsi, notamment, il a l'obligation de fournir certaines informations à la personne concernée, de lui garantir un droit d'accès à ses données; une obligation de mise en oeuvre de mesures techniques et d'organisation afin d'assurer un certain niveau de sécurité; une obligation de notification à l'autorité de contrôle;...[22]. Le responsable du traitement sera tenu de réparer le préjudice subi en cas de dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la directive, à moins de prouver que le fait ayant causé le dommage ne lui est pas imputable[23].

Le responsable du traitement peut traiter les données lui-même ou les faire traiter par d'autres personnes, membres de son personnel ou par un "sous-traitant".

---

[17] Voir considérant 15 de la directive.

[18] Voir l'exposé des motifs de la proposition modifiée de directive du Conseil, COM (92) 422 final - SYN 287, Bruxelles 15 octobre 1992, page 10

[19] Directive, article 2.d. *in fine* : "Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire".

[20] Il n'est toutefois pas tout à fait clair de savoir ce que l'on entend par "les moyens" du traitement. S'agit-il des moyens techniques ou organisationnels?

[21] Voir l'article 4.2. de la directive *supra*.

[22] Ces obligations seront vues en détail aux Chapitres V et VI.

[23] Directive, article 23

## *Section 6 : Le sous-traitant*

Le sous-traitant est défini à l'article 2.e. de la directive comme étant "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement".

La directive prévoit un régime de collaboration très stricte entre le responsable du traitement et son sous-traitant. Le responsable du traitement doit choisir un sous-traitant qui apporte des garanties suffisantes en termes de mesures de sécurité technique et d'organisation relatives aux traitements à effectuer, et veiller au respect de ces mesures[24]. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur la seule instruction du responsable du traitement. Ainsi, le sous-traitant, de même que les personnes agissant sous sa responsabilité, ne peuvent traiter les données à caractère personnel que sur instruction du responsable du traitement[25]. En outre, les obligations concernant la sécurité des traitements, telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci. Ce contrat ou acte juridique et les mesures de sécurité à prendre afin de respecter la législation nationale devront être consignés par écrit ou sous toute autre forme équivalente[26].

Comme nous l'avons déjà précisé à propos du responsable du traitement, toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute autre action incompatible avec les dispositions nationales prises en application de la directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi. Le responsable pourra toutefois s'exonérer partiellement ou totalement s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. La directive semble, dès lors, instaurer en ce qui concerne le responsable du traitement un régime de responsabilité par le fait des choses, les choses étant en cette matière les données qui sont sous la garde du responsable. La personne ayant subi un dommage ne devra prouver aucune faute de la part du responsable du traitement. Ce dernier est présumé responsable sauf à prouver que le fait ne lui est pas imputable (force majeure, faute d'autrui,...). Ceci exclut que celui-ci puisse s'exonérer en démontrant l'accomplissement des diligences qui devaient être mis en oeuvre dans le cadre de ses obligations.

La lecture de l'article 23 de la directive, n'exclut donc pas que la responsabilité du sous-traitant soit mise en cause, partiellement ou totalement du fait d'un traitement illicite ou de toute autre action incompatible avec les dispositions nationales prises en application de la directive. Cela sera le cas notamment si le responsable du traitement

---

[24] Directive, article 17.2.
[25] Directive, article 16
[26] Directive, article 17.3 et 17.4.

parvient à prouver que le fait ayant provoqué le dommage ne lui est pas imputable (le sous-traitant a agit en dehors des instructions du responsable du traitement, par exemple). Toutefois, il nous semble que dans le cas de responsabilité du sous-traitant, la personne concernée devra prouver la faute de ce dernier. Dans ce cas la "liciété" du traitement pourrait découler de la preuve, par le sous-traitant, de toute la diligence attendue de lui dans le cadre de dispositions prévoyant des obligations de moyens à sa charge (sécurité des données,...) et plus généralement si aucune faute ne peut lui être imputée.

## CHAPITRE III : COMMUNICATION DES DONNÉES

La notion de "communication" n'est pas définie en tant que telle dans le texte de la directive. C'est donc par le biais de la définition du "destinataire" telle que définie à l'article 2.g. que l'on peut préciser la notion. En effet, le "destinataire" est toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non de tiers[27]. La communication a lieu, dès lors, dès qu'il y a transmission des données à une autre personne, que celle-ci soit une personne tierce ou soit sous-traitant, responsable du traitement, ou les personnes travaillant sous leur autorité directe.

La directive ne prévoit pas de régime spécifique pour la communication des données. Toutefois, la communication peut être considérée comme un traitement à part entière (opération poursuivant une finalité déterminée), et implique dès lors le respect de l'ensemble des dispositions de la directive applicables aux traitements de données à caractère personnel.

## CHAPITRE IV : FLUX TRANSFRONTIÈRES DE DONNÉES

Tout comme le rapport précédent, cette étude se doit d'envisager la question des flux transfrontières de données à destination de pays tiers à la Communauté européenne. En effet, si S.W.I.F.T. devait être considéré comme responsable de traitement, fût-ce pour une partie de ses activités, il devrait bien entendu respecter le prescrit européen en la matière. En outre, même en-dehors de cette hypothèse, les membres européens affiliés au réseau peuvent certainement être considérés comme responsables de traitement, et sont donc soumis aux règles de la directive concernant les flux transfrontières de données. L'activité de S.W.I.F.T. permettant d'effectuer ces

---

[27] Par "tiers", l'article 2.f. de la directive entend "la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter des données".

transferts de données, S.W.I.F.T. subira donc vraisemblablement certaines conséquences indirectes de l'existence de ces règles.

Venons-en au système mis en place par la directive. Le texte européen affirme explicitement son intention de promouvoir les libertés et droits fondamentaux des personnes, notamment leur vie privée[28]; pour atteindre cet objectif, une limitation doit pouvoir être imposée aux flux transfrontières de données. Sans ces dispositions, le contournement des règles de la directive serait trop aisé pour les responsables de traitements qui feraient effectuer les traitements dans des États moins protecteurs (ou "data havens").

L'approche retenue par le législateur communautaire est l'établissement d'une règle générale (article 25), suivie d'un certain nombre de dérogations (article 26).

## ***Section 1 : Règle générale (article 25)***

L'article 25 (1) dispose que les États membres "prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement ou destinées à faire l'objet d'un traitement ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat".

La notion d'adéquation suscite toujours controverses et interrogations dans tous les milieux concernés. Un des points les plus discutés concerne la différence entre les concepts de protection adéquate et de protection équivalente tel qu'il était proposé par la Convention n°108, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractères personnels[29]. Contrairement à ce qui est parfois soutenu, le requis de protection adéquate ne nous paraît pas en soi moins exigeant que celui de protection équivalente, d'autant que les régimes des deux textes sont différents: la directive prévoit une *interdiction de principe* sauf s'il existe une protection adéquate, alors que la Convention 108 prévoit une simple *faculté d'interdire* les transferts s'il n'existe pas de protection équivalente, mais ne prévoit pas de régime impératif pour les transferts vers les pays non signataires.

Cela étant, l'évaluation de l'adéquation du niveau de protection offerte par le pays tiers reste délicate; elle doit se faire au cas par cas et prendre en compte les caractéristiques du transfert examiné, ce qui signifie que, pour un même pays tiers, le niveau de protection peut être jugé adéquat dans certains cas mais pas dans d'autres. La

---

[28] Directive, article 1 et deuxième Considérant.
[29] Ci-après, Convention 108.

directive ne mentionne que quelques éléments d'appréciation, en son article 25 (2)[30]; cette énumération n'est certainement pas exhaustive. Il s'agit de la nature des données, de la finalité et la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit générales ou sectorielles en vigueur dans le pays tiers en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées.

L'évaluation du niveau de protection du pays tiers suppose dès lors une approche "fonctionnelle": ce que l'on tente de retrouver dans le pays tiers n'est pas un système de protection identique à celui mis en place au sein de la Communauté européenne, mais bien un ou des mécanismes qui assurent adéquatement la protection des données personnelles d'un transfert considéré, compte tenu des caractéristiques du dit transfert. Il s'agira donc de faire une analyse des risques entraînés par un flux pour les personnes concernées, et ensuite, de tous les éléments qui, dans le pays tiers, répondent à ces risques. Une attention particulière doit être portée à la mise en oeuvre pratique d'éventuels instruments de protection des données; cette mise en oeuvre (et les droits en résultant pour les personnes fichées) est extrêmement difficile à évaluer, et nécessite une bonne connaissance des traditions juridiques du pays tiers. On pense par exemple à la question du poids à accorder à la présence de codes de conduite dans le pays tiers (force obligatoire, possibilité d'en invoquer le contenu devant les tribunaux comme "règles de l'art", retentissement dans le public d'éventuelles défaillances du responsable,...).

L'analyse et la prise de décision quant à l'autorisation d'un transfert reposeront d'abord sur les États membres. La directive ne précise pas plus avant quelle instance sera chargée de l'évaluation. Si l'État membre estime le niveau de protection adéquat, il doit normalement autoriser le transfert. Dans le cas contraire, les États membres et la Commission doivent "s'informer mutuellement"[31].

Des mécanismes fédérateurs existent afin d'unifier les réactions des États membres: la Commission peut en effet établir des "black lists" de pays tiers dont la protection est considérée comme inadéquate en tout état de cause (quel que soit le flux considéré). Dans ce cas, les États membres doivent prendre des mesures afin d'empêcher tout transfert vers les pays en question[32]. La Commission peut engager des négociations avec ces pays afin de remédier à cette situation. Elle peut également établir

---

[30] Article 25 (2): "Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou une catégorie de transferts de données; en particulier, sont prises en considération [voir énumération ci-dessus]".

[31] Directive, article 25 (3).

[32] Directive, article 25 (4)

des "white lists" de pays tiers considérés comme assurant une protection adéquate, par exemple en raison de leur législation interne ou de leurs engagements internationaux[33].

La constitution de listes blanches ou noires doit se faire selon la procédure prévue par l'article 31 (2) de la directive, ce qui signifie que la Commission prendra les mesures en fonction des avis émis par le Comité institué par cet article, constitué de représentants des États membres et de la Commission. Il existe un risque que les décisions soient de nature politique (ainsi, on peut douter que les États membres décident de faire déclarer inadéquate la protection assurée par un partenaire commercial puissant comme les États-Unis, par exemple).

## *Section 2. Les dérogations (Article 26)*

### 2.A. Dérogations spécifiques

L'article 26(1) prévoit certaines conditions auxquelles un transfert de données personnelles vers un pays n'assurant pas une protection adéquate peut malgré tout être autorisé. Ces dérogations ont été prévues pour répondre aux inquiétudes de certains secteurs, et, en pratique, pourront être largement appliquées dans les secteurs bancaire et du tourisme en particulier. Notons que ces dérogations peuvent voir leur effet limité; la rédaction de l'article 26(1)[34] laisse penser que les États membres peuvent adopter des législations selon lesquelles le transfert reste interdit malgré la présence de l'une ou l'autre des dérogations.

Parmi les dérogations spécifiques prévues à l'article 26(1), les suivantes pourraient être d'application dans le cadre des activités de S.W.I.F.T. ou de ses affiliés.

*a) la personne concernée a indubitablement donné son consentement au transfert envisagé.*

Notons que la personne concernée ne doit pas simplement donner son consentement au traitement de ses données, mais bien au transfert lui-même. Le consentement doit être informé[35], ce qui signifie dans ce contexte que la personne concernée doit être mise au courant des risques spécifiques entraînés pour elle par un

---

[33] On peut se demander quels engagements internationaux sont visés ici. Si la ratification de la Convention 108 du Conseil de l'Europe paraît constituer une présomption de protection adéquate (entre autre dans la mesure où elle implique que les pays en question ait adopté une législation protectrice), il n'en est sans doute pas de même pour l'adhésion aux Lignes Directrices de l'OCDE, dont la force contraignante est moindre.

[34] "Par dérogaton à l'article 25 et *sous réserve de dispositions contraires de leur droit national régissant des cas particuliers*, les Etats membres prévoient qu'un transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2 peut être effectué à condition que (...)."

[35] Directive, article 2(h): le consentement est "toute manifestation de volonté libre, spécifique et informée (...)".

transfert de ses données personnelles vers un pays n'assurant par définition pas une protection adéquate. En outre, le consentement doit être indubitable, c'est-à-dire clair et non équivoque. On peut s'interroger sur la validité d'un consentement donné sous forme d'adhésion à des conditions générales, sans porter spécifiquement sur un transfert particulier.

*b) Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée.*

*c) Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.*

Ces dérogations sont, comme la précédente, exigeantes: il faut que le *transfert* lui-même soit nécessaire, et non le traitement. Dès lors, la délocalisation de la gestion des ressources humaines d'une société pourrait ne pas répondre à ce critère, par exemple (il est nécessaire de traiter ces données, mais, en soi, le transfert vers le pays tiers ne paraît pas nécessaire à l'exécution du contrat).

Toutefois, ces deux dérogations nous paraissent pouvoir être le plus souvent utilisées dans le cadre des activités du secteur bancaire: la plupart des transferts de données personnelles sont en effet nécessaires à l'exécution d'un contrat conclu entre le banquier et son client, ou encore en faveur du client (exécution de virements,...).

La personne concernée devra être informée des risques entraînés par un transfert de ses données vers un pays n'assurant pas une protection adéquate, car il nous semble que cette information est nécessaire "pour assurer à [son] égard un traitement loyal des données"[36]. En effet, si le transfert est nécessaire à l'exécution d'un contrat, une utilisation totalement différente des données peut être faite dans le pays tiers.

Les exceptions suivantes prévues à l'article 26(1) sont la "sauvegarde d'un intérêt public important, la constatation, l'exercice ou la défense d'un droit en justice (d), la sauvegarde de l'intérêt vital de la personne concernée (e), ou le transfert au départ d'un registre public (...) destiné à l'information du public et ouvert à la consultation du public (...) (f). Ces dérogations ne nous paraissent pas devoir être développées ici, dans la mesure où elles nous semblent peu utilisables dans le cadre des activités du réseau S.W.I.F.T.

---

[36] Directive, articles10 (c) et 11.1 (c).

## 2.B. Les "clauses contractuelles appropriées"

Dans le cas où le pays tiers n'assure pas une protection adéquate, et que les dérogations prévues à l'article 26(1) ne sont pas d'application, un transfert de données à caractère personnel vers le dit pays tiers peut néanmoins être autorisé, "lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées".

L'article 26 (2) prévoit alors une procédure d'information de la Commission et des autres États membres par l'État membre accordant une telle autorisation. En cas d'opposition exprimée par un autre État membre ou par la Commission (opposition "dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes"[37]), la Commission doit prendre des mesures appropriées après avoir pris l'avis du Comité consultatif établi par l'article 31 de la directive. Ces mesures appropriées peuvent consister en l'interdiction du transfert.

La question qui se pose d'emblée est de savoir si l'existence de clauses contractuelles entre l'exportateur et le destinataire des données peut assurer à la personne concernée une protection suffisante. Quel que soit le contenu de ces clauses, le contrat est pour les personnes concernées une *res inter alios acta*, qu'ils ne peuvent en principe invoquer en cas de manquement. Tout autre est la situation où les dites clauses sont rendues opposables aux personnes concernées par leur inclusion dans des conditions générales, par exemple. A part dans cette hypothèse, l'individu concerné ne peut faire valoir aucun droit ni introduire de recours dans le cas d'une utilisation erronée ou abusive de ses données.

Dès lors, si l'on veut que les mesures contractuelles fournissent une protection adéquate, il semble prudent d'introduire dans le contrat des dispositions garantissant à la personne concernée la possibilité d'invoquer ces clauses, et de les opposer à l'exportateur des données[38] (qui, par hypothèse est plus facile à localiser, puisqu'il est situé sur le même territoire que la personne concernée). Sans cette possibilité, des clauses contractuelles ne nous semblent pas suffisantes au regard même de l'article 26 (2), puisqu'elles doivent offrir des garanties suffisantes "au regard de la protection de la vie privée (...) et de l'exercice des droits correspondants".

---

[37] Directive, article 26 (3)

[38] Ce mécanisme est développé par J. Reidenberg, in "Setting standards for Fair Information Practice, Iowa Law Review, March 1995, Vol.80, N°3.

## CHAPITRE V : APPLICATION DES PRINCIPES RÉGISSANT LA DIRECTIVE

Le responsable du traitement est la personne qui a la charge principale du respect des obligations prévues par la directive. Cette partie a pour but de passer en revue les obligations, qui doivent être prévues dans les législations des États membres à charge des responsables du traitement.

### *Section 1 : Le principe de finalité*

Avant de procéder à l'analyse proprement dite des principes énoncés par la directive, il est utile de se pencher sur l'articulation des dispositions du chapitre II de la directive, intitulé "les conditions générales de licéité des traitements de données à caractère personnel"[39]. L'article 6 énonce des principes relatif à la qualité des données traitées et pose les principes de légitimité et de conformité. L'article 7 précise les facteurs limitatifs de légitimation des traitements de données à caractère personnel : tout traitement qui ne peut trouver son fondement dans l'un des principes énoncés à l'article 7 ne peut être effectué. Les considérants de la directive semblent poser l'hypothèse d'une application cumulative des articles 6 et 7[40]. Le traitement ne sera pas d'office considéré comme "légitime" du seul fait qu'il trouve son fondement dans un des facteurs stipulés à l'article 7. Dès lors, les autorités nationales pourront toujours contester la légitimité du traitement[41].

#### 1.A. Principe de finalité légitime

L'article 6.1.a et b de la directive traduit le principe de légitimité du traitement. Les données doivent être "collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités". Les données doivent être traitées de manière "loyale et licite". Un traitement loyal suppose un traitement transparent, pour des finalités connues et explicites aux yeux de la personne conernée. Un traitement licite suppose que les conditions générales de licéité du traitement énoncées au chapitre II de la directive, soient respectées.

Le but poursuivi par le traitement doit être déterminé et explicite. Le fondement de cette règle réside dans une exigence de transparence du projet. La poursuite d'une

[39] L'article 5 de la directive stipule "Les États membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites".

[40] Selon le considérant 28, tout traitement de données à caractère personnel doit être effectué licitement et loyalement à l'égard des personnes concernées; qu'il doit en particulier porter sur des données adéquates, pertinentes et non excessives au regard des finalités poursuivies et que ces finalités doivent être explicites et légitimes. Par ailleurs, le 30ème considérant précise que pour être licite le traitement de données à caractère personnel doit "en outre" être fondé sur l'un des critères énoncés à l'article 7.

[41] Il n'empêche que certains facteurs énoncés à l'article 7, tels le consentement de la personne concernée, pourront néanmoins influencer les autorités de contrôle dans leur appréciation de la légitimité du traitement.

finalité secrète ou imprécise est donc exclue. Le responsable du traitement sera tenu de divulguer la finalité du traitement à la personne concernée[42] et de la notifier à l'autorité de contrôle[43].

Chaque finalité doit être légitime[44]. La directive ne définit pas ce qu'elle entend par une finalité légitime. Il appartiendra donc aux autorités de contrôle de chaque pays membre de déterminer quand un traitement de données à caractère personnel poursuit une finalité dite "légitime".

Le changement de la finalité n'est pas condamnable a priori, pourvu que la modification ne soit pas incompatible avec la finalité annoncée au départ. En particulier, la directive prévoit qu'un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas incompatible pour autant que les États membres prennent des garanties appropriées[45].

### 1.B. Principes relatifs à la légitimation des traitements de données

Les principes exposés à l'article 7 de la directive constituent les fondements du traitement de données à caractère personnel. Les États membres devront prévoir que le traitement de données à caractère personnel ne peut être effectué que si :

*a) La personne concernée a donnée indubitablement son consentement[46];*

Le consentement de la personne concernée est défini comme étant "toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement" [47].

Le consentement doit être libre c'est à dire qu'il ne doit pas être donné sous pression.

Par ailleurs, le consentement doit être spécifique c'est à dire qu'il doit être relatif à un traitement précis de données relatives à la personne concernée par un responsable déterminé et pour des finalités déterminées. Ainsi toute modification de la finalité d'un traitement exige un consentement nouveau de la personne concernée.

Le consentement doit être informé. Cette condition trouve son pendant dans l'obligation d'information du responsable du traitement vis à vis de la personne concernée[48].

Le consentement doit être donné de manière indubitable: il ne peut y avoir aucun doute relatif à l'existence ou l'étendue de ce consentement au traitement des données.

---

[42] Directive, articles 10 et 11 (obligation d'information)
[43] Directive, article 18 (obligation de notification)
[44] Directive, article 6.b.
[45] Directive, article 6
[46] Directive, article 7.1.a.
[47] Directive, article 2.h.
[48] Voir *infra*

*b) Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celui-ci*[49]*;*

*c) Le traitement est nécessaire pour le respect d'une obligation légale à laquelle le responsable du traitement est soumis*[50]*;*

*d) Le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée*[51]*;*

*e) Le traitement "est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées";*

*f) Le traitement "est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et les libertés fondamentaux de la personne concernée"*[52].

Cette disposition implique non seulement que le responsable poursuive un intérêt considéré comme "légitime" par les autorités de contrôle, mais également que l'on procède à un équilibre des intérêts en jeu. Il en résulte qu'une finalité violant les intérêts individuels sans se fonder sur un intérêt supérieur doit être considérée comme illégitime. Une finalité serait de même illégitime si la poursuite de l'intérêt du ficheur implique pour l'individu des risques disproportionnés par rapport à ce qui est strictement nécessaire.

## ***Section 2 : Principes régissant les catégories particulières de données***

Le traitement des données qui sont susceptibles par leur nature de porter atteinte aux libertés fondamentales ou à la vie privée (dites "sensibles") est interdit, sauf s'il tombe sous l'une des dérogations prévues dans l'article 8[53]. Par données sensibles l'article 8 de la directive entend "les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle".

---

[49] Directive, article 7.b.

[50] Directive, article 7.c.

[51] Directive, article 7.d.

[52] Directive, article 7.f.

[53] Les dérogations prévues à l'article 8 s'appliquent sans préjudice des conditions générales de licéité d'un traitement prévues aux articles 6 et 7.

## *Section 3 : Principes relatifs à la qualité des données*

La directive prévoit, à l'article 6.1. certaines exigences en ce qui concerne la qualité de données à caractère personnel. Il incombe au responsable du traitement de veiller au respect de ces requis[54].

L'article 6.1.c. de la directive prévoit que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement.

Cette disposition fait référence au concept de conformité des données. Contrairement au principe de légitimité, le principe de conformité des données ne se situe plus au niveau de l'existence même du traitement mais du contenu de celui-ci : une finalité légitime et déclarée n'autorise pas d'elle-même l'utilisation de n'importe quelle donnée. Le principe de conformité implique que les données utilisées soient adéquates, pertinentes et non excessives par rapport à la finalité déclarée et légitime. L'adéquation et la pertinence de la donnée ne visent rien d'autre qu'une liaison nécessaire et suffisante de l'information au but poursuivi par le traitement.

Par ailleurs, en vertu de l'article 6.1.d, les données doivent être exactes et si nécessaires mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.

Enfin, les données ne doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités[55].

# CHAPITRE VI : OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

## *Section 1 : Obligation d'information (articles 10 et 11)*

L'information de la personne concernée est l'une des obligations imposées au responsable du traitement. Le responsable du traitement est tenu d'informer la personne concernée de l'identité du responsable du traitement, et, le cas échéant, de son représentant; des finalités du traitement auquel les données sont destinées et de toute information supplémentaire dans la mesure où, compte tenue des circonstances particulières dans lesquelles les données sont collectées, ces informations sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des

---

[54] Directive, article 6.2.
[55] Directive, article 6.1.e.

données. Ces dernières informations concernent, notamment, les destinataires ou catégories de destinataires des données, le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences d'un défaut de réponse, et l'existence d'un droit d'accès aux données les concernant et de rectification de ces données.

En cas de collecte de données auprès de la personne concernée, l'information se fera au moment même de la collecte[56]. Lorsque les données n'ont pas été collectées auprès de la personne concernée cette information ainsi que l'information sur les données ou les catégories de données traitées devra être fournie par le responsable du traitement ou son représentant, soit dès l'enregistrement des données ou, si une communication des données à un tiers est envisagée, au plus tard lors de la première communication des données[57].

L'article 13 permet aux États membres de prendre des mesures législatives afin de limiter ce droit à l'information lorsque les données n'ont pas été collectées auprès de la personne concernée, et ceci notamment en vue de sauvegarder la protection de la personne concernée.

Notons que le devoir d'information par le responsable du traitement prévu à l'article 11 de la directive ne s'applique pas lorsque, en particulier pour un traitement à finalité statistique ou de recherche scientifique, l'information de la personne concernée se révèle impossible ou implique des devoirs disproportionnées, ou si la législation prévoit expressément l'enregistrement ou la communication des données. Dans ces cas, les États membres prévoient des garanties appropriées[58].

## ***Section 2 : Confidentialité et sécurité des traitements***

L'article 16 dispose que "toute personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en vertu de dispositions légales".

Par ailleurs, l'article 17 prévoit, que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et la nature des données à protéger.

---

[56] Directive, article 10

[57] Directive, article 11

[58] Directive, article 11.2 de la directive

## *Section 3 : Respect des droits de la personne concernée*

La directive prévoit un certain nombre de droits pour la personne concernée par les données à caractère personnel. Il incombe au responsable du traitement de veiller à la mise en oeuvre et au respect de ces droits.

### 3.A. Droit d'accès (Article 12)

L'article 12.1. permet à la personne concernée d'obtenir notamment "la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiqués" et "la communication, sous forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données."

### 3.B. Droit de rectification (article 12.2.et 12.3)

Le droit de rectification tel qu'il est prévu dans la directive consiste dans le droit d'obtenir du responsable du traitement "la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données" ainsi que "la notification aux tiers auxquels les données ont été communiquées de toute rectification, effacement ou verrouillage effectué conformément au point 2, si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné".

### 3.C. Droit d'opposition (article 14)

Ce droit est celui "au moins dans les cas visés à l'article 7 points e) et f) de s'opposer à tout moment pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire dans le droit national. En cas d'opposition justifiée, le traitement mis en oeuvre par le responsable du traitement ne peut plus porter sur ces données".

### 3.D. Le droit de ne pas être soumis à une décision individuelle automatisée (article 15)

La directive prévoit, en son article 15, que les États membres devront reconnaître à toute personne, le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité (tels que son comportement, son rendement professionnel, son crédit, sa fiabilité,...).

Trois conditions doivent donc être réunies afin qu'un individu puisse invoquer ce droit. Premièrement, il faut qu'une décision soit prise à son égard, décision produisant des effets juridiques ou l'affectant de manière significative. Deuxièmement, cette décision doit résulter uniquement du traitement automatisé lui-même, sans intervention humaine. Enfin, le traitement doit être destiné à évaluer certains aspects de la personnalité. La décision sur la possibilité pour un individu de retirer de l'argent auprès d'un distributeur automatique d'après le solde de son compte, par exemple, n'est pas une décision ayant pour but d'évaluer des aspects de la personnalité et ne tombe pas sous le coup de l'article 15.

L'article 15 prévoit, toutefois, des exceptions à l'interdiction de prendre des décisions individuelles automatisées notamment quand la décision est prise dans le cadre de la conclusion ou l'exécution d'un contrat, à la condition que la demande introduite par la personne concernée ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime. Une telle décision est également permise si elle est autorisée par une loi garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

A la lecture de ce que nous venons de dire, il ne semble pas que S.W.I.F.T., dans le cadre actuel de ses activités, soit amené à prendre des décisions individuelles automatisées destinées à évaluer la personnalité d'une personne physique. En effet, S.W.I.F.T. ne s'intéresse en principe pas au contenu même du message financier (est-ce que Monsieur X était autorisé à effectuer la transaction financière) transmis entre institutions financières, mais ne fait qu'assurer la transmission du message lui-même.

## ***Section IV. Notification à l'autorité de contrôle***

L'article 18 dispose que "les États membres prévoient que le responsable du traitement, ou le cas échéant son représentant, doit adresser une notification à l'autorité de contrôle [de son pays] préalablement à la mise en oeuvre d'un traitement (...)".

Le contenu de cette notification doit être déterminé par les États membres, mais elle doit contenir au moins le nom et l'adresse du responsable du traitement, la ou les finalités du traitement, la description des catégories de personnes concernées et des données ou catégories de données s'y rapportant, des destinataires ou catégories de destinataires auxquels les données sont susceptibles d'être communiquées, des transferts de données envisagés à destination de pays tiers, et d'une description générale "permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement" (article 19).

Les États membres peuvent prévoir dans certains cas des simplifications, prévues à l'article 18 §2-5 (dérogations à l'obligation de notification).

# PARTIE II : APPLICATION A S.W.I.F.T.

L'objet de cette partie est de déterminer dans quelle mesure les dispositions de la directive s'appliquent au réseau S.W.I.F.T. dans le cadre de ces services de transmission de messages financiers (FIN).

Rappelons tout d'abord que cette étude, tout comme la précédente, est consacrée aux traitements de données à caractère personnel nécessaires à l'accomplissement du service proposé par S.W.I.F.T., à savoir, la transmission de messages financiers. Nous ne nous traiterons donc pas des fichiers classiques détenus par S.W.I.F.T. comme par la majorité des entreprises, tel le fichier des membres de son personnel; pour ces derniers, en effet, la directive est entièrement d'application.

## CHAPITRE I : LES DONNÉES CONTENUES DANS LES MESSAGES

### *Section 1 : Définitions*

#### 1.A. Données à caractère personnel

Nous renvoyons ici aux conclusions de la précédente étude effectuée pour S.W.I.F.T.[59] Il ne fait aucun doute que les messages S.W.I.F.T. contiennent des données à caractère personnel. Le message "MT 100" en est un exemple[60]: on y trouve bien la référence à une personne identifiée ou identifiable aux termes de l'article 2.a. de la directive.

De même un "broadcast message"[61] peut contenir des données à caractère personnel. Ceci sera notamment le cas dans le message intitulé "change of officers" informant les utilisateurs du changement de nom de la personne de contact dans une institution financière.

#### 1.B. Traitement

La définition du traitement a encore été étendue par rapport au projet de directive, comme on l'a vu dans la partie I de la présente étude (voir Chapitre II, Section 3, "Le traitement").

---

[59] Page 24.

[60] Voir référence et exemple tiré du User Handbook, dans étude précédente, p.25.

[61] A savoir les messages envoyés par S.W.I.F.T. aux utilisateurs ou groupes d'utilisateurs, soit d'initiative soit sur base d'une demande par un utilisateur.

Le réseau S.W.I.F.T. se charge pour ses membres[62] de l'utilisation et la mise en oeuvre des moyens nécessaires pour la "télécommunication, la transmission et l'acheminement"[63] de messages financiers. Il ne fait aucun doute que S.W.I.F.T. exerce un traitement au sens de la directive, ce traitement consistant principalement en enregistrement et communication de données[64]. En effet, l'enregistrement et la communication de données à caractère personnel sont des opérations inhérentes à la fonction première du réseau S.W.I.F.T., à savoir la transmission de messages financiers. En outre, le bon fonctionnement du réseau implique le stockage des messages. Afin de garantir au transfert des messages une fiabilité maximale, les messages sont archivés au niveau du Slice Processor[65]. Ce stockage des messages s'inscrit dans la finalité même du service rendu[66].

### 1.C. Responsable du traitement

Comme nous l'avons déjà vu, le texte de la directive désigne le responsable du traitement comme le destinataire principal des obligations découlant de la directive afin de faciliter la reconnaissance de droits dans le chef des personnes concernées par les données. Si l'idée d'élire un responsable unique paraît être la plus adéquate au niveau de la protection accordée, reste le problème de l'identification de cet interlocuteur. Cette idée de responsable unique qui définit *les finalités et les moyens* du traitement est mal adaptée à la réalité d'un réseau caractérisé par un éclatement des lieux de traitement et une pluralité d'intervenants.

Il est difficile, d'une part, de déterminer qui décide des finalités d'un traitement dans le cadre d'un réseau de transmission dédié à l'accomplissement d'un service particulier. Est-ce l'utilisateur qui décide de communiquer les informations via ce réseau de communication plutôt que par un autre moyen, ou est-ce le fournisseur du service de transmission qui en établit les fonctions?

D'autre part, le deuxième critère d'identification du responsable du traitement, fondé sur la détermination des moyens du traitement pose également des difficultés d'application. L'utilisateur qui confie un message au fournisseur du service de

---

62 "For the collective benefit of the Members of the Company", Article 3§1 des Corporate Rules, Policy, November 1996

63 Notre traduction de l'article 3§1 des Corporate Rules, op. cit.

64 Rappelons que, pour qu'il y ait traitement, il n'est pas nécessaire que l'ensemble des opérations visées à l'article 2.b. de la directive soit effectué; il suffit que l'une d'entre elles soit mise en oeuvre dans un but déterminé.

65 "Two copies of each message are stored on two seperate storage media. If a system failure occurs, input messages already acknowledged by the system are automatically retrieved from either the primary storage media or its backup", Chapter 12 Overview of Message Flow, FIN Service Description, Policy and Operations, November 1996, p.93.

66 Signalons toutefois que les données à caractère personnel doivent être "conservées sous une forme permettant l'identification des personnes pendant une période n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement", Article 6.1.e. de la directive.

transmission ne détermine pas les moyens physiques de la transmission, et pourtant il choisit de communiquer via un réseau plutôt que par un autre moyen de communication et également de s'adresser à tel réseau en particulier. Faut-il donc considérer que S.W.I.F.T. détermine les moyens du traitement, ou qu'il *est* le moyen, choisi par l'affilié pour transmettre le message?

Les considérants de la directive, apportent une solution possible au problème posé dans le cadre de réseau de télécommunications ou de courrier électronique[67]. Ainsi, dans le cas d'une transmission d'un message contenant des données à caractère personnel via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme le responsable du traitement de données à caractère personnel contenues dans le message. Les considérants précisent toutefois, que les personnes qui offrent le service seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service[68]. Selon nous l'idée sous-tendant ce considérant était probablement liée au fait que le service de transmission traite les données à caractère personnel non pas en tant que telles mais en tant que formant partie du message en lui-même. Dans la plupart des cas, d'ailleurs, elle n'accède même pas au contenu même du message.

Ces mêmes arguments pourraient être mis en avant en ce qui concerne le service de transmission de message qu'offre S.W.I.F.T. à ses clients. En effet, selon la définition même du service, FIN est un service de stockage et d'envoi des messages entre institutions financières[69]. Les utilisateurs y trouvent un moyen efficace, sur et rapide d'envoyer des messages financiers aux autres participants d'un réseau de télécommunication géré par la société S.W.I.F.T. Le réseau se voit donc attribué une mission de communication d'un message déjà préétabli par l'institution émettrice et ne se charge que de cette transmission sans se préoccuper du contenu même du message vis à vis duquel il reste entièrement neutre.

Un deuxième argument peut être soulevé afin de ne pas qualifier S.W.I.F.T. comme le responsable du traitement en ce qui concerne la transmission de messages contenant des données à caractère personnel. La qualification de responsable du traitement, nous l'avons déjà vu, implique le respect d'une série d'obligations, notamment de qualité des données, et oblige le responsable à fournir un droit d'accès à la personne concernée à ses propres données. Ces obligations, dans leur nature même,

---

[67] Voir Considérant 47. Le problème n'étant plus posé dans le texte de la directive elle-même, la question reste de savoir le poids que l'on peut accorder aux considérants d'une directive.

[68] Nous songeons, par exemple, au traitement des données à des fins de facturation du service de transmission ou de traçage des transmissions à des finalités de statistiques (cfr. *infra* Partie II et III).

[69] Article 1.2. The FIN Service, FIN Service Description, op. cit.

impliquent que le responsable ait lui-même un accès et une prise de connaissance des données. Dans le cas de S.W.I.F.T. nous avons conclu que même si S.W.I.F.T. disposait des moyens pour accéder aux données à caractère personnel contenues dans les messages transmis, S.W.I.F.T. ne prenait pas connaissance de celles-ci. Or, qualifier S.W.I.F.T. de responsable du traitement aboutirait à créer un espèce de "droit de regard" de S.W.I.F.T. sur les données à caractère personnel en vertu de son obligation de contrôle de la qualité des données et de l'obligation d'assurer un droit d'accès pour la personne concernée.

Qualifier S.W.I.F.T. de responsable du traitement aurait un effet pervers, absolument contraire à la protection recherchée, puisqu'elle l'amènerait à prendre connaissance de données qui sont a priori sans intérêt pour lui ! En outre, la mise sur pied d'un droit d'accès et de rectification crée un risque supplémentaire pour les données (plus de manipulation des données, archivage plus long,...).

Il y a donc ici une "balance des intérêts" à effectuer: il nous semble que la protection des données personnelles contenues dans les messages S.W.I.F.T. est, paradoxalement, mieux assurée si l'on ne considère pas S.W.I.F.T. comme le responsable du traitement.

Il faut, dès lors, envisager une autre qualification pour S.W.I.F.T.: celle de "sous-traitant" correspond mieux au rôle joué par cette société.

### 1.D. Sous-traitant

Comme nous l'avons déjà précisé, le sous-traitant au sens de l'article 2.e. de la directive est une personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite les données à caractère personnel "pour le compte du responsable du traitement". Or nous pouvons lire à l'article 3 des "Articles of Association"[70], que l'objet de S.W.I.F.T. est de traiter des messages financiers et pouvant contenir des données à caractère personnel au bénéfice collectif des membres de la société[71]. Il semble dès lors qu'il faille distinguer entre le société S.W.I.F.T. en elle-même et les membres utilisateurs qui la composent et qui sont eux-mêmes à l'origine de l'envoi d'un message financier. Seuls ces derniers décident de la finalité et des moyens du traitement et pourront être qualifiés de responsables du traitement[72].

La qualification de S.W.I.F.T. comme sous-traitant implique l'existence d'un contrat ou acte juridique entre S.W.I.F.T. et les membres qui prévoit notamment que S.W.I.F.T., ainsi que tout autre personne agissant sous son autorité, ne pourra agir que

---

[70] Op. cit.

[71] Les "Membres" étant toutes les organisations admis dans le groupe selon la procédure prévue par les "Articles Of Association"

[72] Les membres pourront effectuer cette détermination seuls ou conjointement, selon les termes mêmes de l'article 2 de la directive.

sur seule instruction du responsable du traitement[73]. Par ailleurs, cet acte ou contrat devra prévoir que les obligations relatives aux mesures de sécurité prévues à l'article 17.1. de la directive incombent également au sous-traitant.

En matière de sécurité des traitements l'article 17.1. de la directive prévoit que des mesures techniques et d'organisation appropriées doivent être adoptées pour protéger les données à caractère personnel contre la destruction accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés et de la nature des données à protéger.

Les mesures de sécurité à adopter résultent d'une équation à trois variables : les risques du traitement (y compris l'intérêt que peuvent avoir des tiers dans l'accès non autorisé aux données et ce particulièrement dans le cas où le traitement comporte des transmissions par réseau), la nature des données (données à caractère personnel "sensibles" ou non) et la disponibilité et le coût de mesures techniques capables de pallier les risques. Les mesures adoptées par S.W.I.F.T. peuvent être d'ordre technique (introduction de codes d'accès, chiffrement de certains documents,...) ou organisationnels (verrouillage de certains ordinateurs, accès contrôlé aux locaux,...).

Si le responsable du traitement est le premier responsable pour la réparation de tout préjudice subi par la personne concernée par les données à caractère personnel, S.W.I.F.T., en tant que sous-traitant, n'est cependant pas exempt de toute responsabilité. En effet, dans le cas où il outrepasse les pouvoirs qui lui sont attribués dans le contrat qui le lie au responsable du traitement, il sera non seulement responsable contractuellement envers le responsable du traitement mais il pourra être tenu de réparer partiellement ou totalement le préjudice subi par suite de son manquement si la victime parvient à prouver une faute qui lui est imputable[74].

## CHAPITRE II : LES DONNÉES GÉNÉRÉES PAR L'UTILISATION DU RÉSEAU S.W.I.F.T.

Si S.W.I.F.T. ne peut être qualifié de responsable du traitement en ce qui concerne les données à caractère personnel contenues dans les messages[75], il n'échappe cependant pas à toute obligation. Nous avons en effet, déjà pu dégager un certain nombre d'obligations et de responsabilités incombant à S.W.I.F.T. en tant que sous-

---

[73] Directive, article 17.3.

[74] Cela n'empêchera toutefois pas S.W.I.F.T. de limiter contractuellement sa responsabilité dans certains cas (cfr. FIN Policy, op. cit. Chapter 4, S.W.I.F.T.'s Liability).

[75] "Message data"

traitant. Par ailleurs, si S.W.I.F.T. peut être qualifié de responsable du traitement sur les données relatives aux utilisateurs et générées par l'utilisation du réseau[76], cela impliquera le respect des obligations incombant aux responsables de traitement. C'est ce qu'il convient d'examiner dans cette partie. On ne vise plus ici les données à caractère personnel contenues dans les messages circulant sur le réseau géré par S.W.I.F.T., mais bien les données à caractère personnel nécessaires au fonctionnement du réseau ou crées par l'utilisation de celui-ci.

Il convient de faire une distinction entre l'application de la proposition de directive spécifique aux télécommunications (Section I), d'une part, et celle de la directive générale d'autre part (Section II).

## ***Section I : La proposition de Directive "télécoms"***[77]

La directive générale relative à la protection des données à l'égard du traitement des données à caractère personnel, a été conçue comme une directive-cadre. Le texte est censé être complété par des dispositions complémentaires, visant à apporter des solutions plus spécifiques dans certains domaines particuliers.

Face aux risques d'atteinte à la vie privée auxquels peuvent donner lieu l'introduction de nouvelles technologies dans les réseaux de télécommunications, la directive télécoms vise à appliquer les principes de la directive générale dans un domaine spécifique et à répondre aux besoins propres aux nouveaux réseaux de télécommunications. Toutefois, contrairement à ce qui était attendu[78], la directive ne s'applique qu'aux réseaux publics de télécommunications, l'amendement du Parlement Européen visant à élargir le champ d'application aux réseaux privés, n'ayant pas été adopté[79].

Par réseau public de télécommunications il faut entendre selon l'article 2.c. de la proposition : "les systèmes de transmission et, le cas échéant, l'équipement de communication et les autres ressources permettant le transport de signaux entre des points de terminaisons définis, par fils, par faisceaux hertziens, par moyens optiques ou par d'autres moyens électromagnétiques, qui sont utilisés en tout ou en partie, pour la fourniture de services de télécommunications accessibles au public". S.W.I.F.T. n'offrant pas un réseau de télécommunication accessible au public mais seulement au

---

76 "Traffic data"

77 Selon la position commune (CE) N° 57/96 arrêtée par le Conseil le 12 septembre 1996 en vue de l'adoption de la directive 96/.../CE du Parlement Européen et du Conseil concernant la protection des données personnelles et la protection de la vie privée dans le secteur des télécommunications (en tenant compte des derniers amendements adoptés lors de la seconde lecture par le Parlement Européen le 16 janvier 1997)

78 Voir étude réalisée par M-H. BOULANGER et Th. LEONARD, p.39.

79 Article 3.1. de la directive télécoms "Services concernées".

groupe que constitue ses membres, il est dès lors raisonnable de dire, qu'en l'état actuel du texte, il ne s'applique pas à S.W.I.F.T.

## *Section 2 : Application de la directive générale*

La directive générale 95/46, examinée dans la première partie de cette étude, reste d'application dans le secteur des télécommunications pour tout ce qui n'est pas spécifiquement couvert par la directive télécoms, notamment pour tous les services de télécommunication privés[80].

Un certain nombre de données à caractère personnel sont nécessaires au fonctionnement du réseau ou sont crées par l'utilisation de celui-ci. Il s'agit de données relatives aux utilisateurs du service pour autant que ceux-ci soient des personnes physiques[81]. Les données collectées par S.W.I.F.T. dans ce cas seront certainement mises en rapport avec l'utilisateur. Nous songeons, par exemple, aux données collectées et traitées par S.W.I.F.T. en vue de la facturation du service fourni (coordonnés de l'utilisateur, le type de message émis, la date et l'heure de la transmission,...). Les informations nominatives sont donc enregistrées et conservées pour des finalités de transmission de messages, de preuve et de facturation des services. Pour autant que les utilisateurs sont des personnes physiques, tous les traitements portant sur ces données sont couverts par la directive.

Dans ce cas, il nous paraît évident que S.W.I.F.T. peut être qualifié de responsable du traitement[82]. En effet, S.W.I.F.T. effectue un certain nombre d'opérations (regroupement des données : nombre de message envoyés, date et durée de la transmission,....) sur des données relatives à une personne identifiable afin de calculer la somme due par cette dernière. S.W.I.F.T. détermine la finalité poursuivie (facturation du service) et les moyens mis en oeuvre pour atteindre celle-ci. Les obligations incombant au responsable du traitement et développées précédemment, incombent dès lors à S.W.I.F.T.

---

[80] Voir considérant 9 de la position commune précitée de la proposition de directive télécoms.

[81] Cette hypothèse nous parait cependant assez peu vraisemblable au regard de la clientèle de S.W.I.F.T. et des services offerts.

[82] Nous renvoyons à ce propos au considérant 47 de la directive générale commentée dans Partie II, chapitre I : "... les personnes qui offrent ces services seront normalement considérées comme responsable du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service".

# Partie III Autres Services

Mise à part l'étude, la création, l'utilisation et la mise en oeuvre des moyens nécessaires pour la communication, la transmission et l'acheminement de messages financiers[83], S.W.I.F.T. peut également, en vertu de l'article 3.2. des Articles of Association, fournir elle-même des produits et services relatifs à son objet avec l'accord du "Board of Directors". En vertu de cette disposition, il est donc permis à S.W.I.F.T. de créer ses propres services et produits pour autant que ceux-ci entrent dans le cadre du service de transmission initial. Il semble donc à première vue que contrairement au service de messagerie initial, ces services ne soient plus offerts pour le compte des membres de S.W.I.F.T., mais qu'ils soient développés par S.W.I.F.T. en tant que telle et pour son propre compte. C'est donc l'application de la directive à deux de ces services que nous allons étudier dans cette partie.

## CHAPITRE I : LE SERVICE FIN COPY

### *Section 1 : Description du service*[84]

Le service FIN Copy établit un mécanisme permettant à un tiers désigné (Banque Centrale, Clearing House,...) de contrôler les transactions financières entre institutions financières. FIN Copy utilise les moyens techniques du service de messagerie FIN en y ajoutant la possibilité de copier automatiquement l'information pour le tiers et ceci à des fins de "clearing", de "netting" ou de règlement de transactions financières. Les opérations s'effectuent donc entre trois entités (l'institution émettrice, l'institution centrale, et l'institution réceptrice) selon un accord préétabli par elles[85].

C'est l'institution émettrice qui décide d'envoyer un message Fin Copy. Dans ce cas, le message est automatiquement intercepté et envoyé à l'institution centrale désignée et ceci

- soit en même temps que l'envoi à l'institution réceptrice (envoi en mode T-Copy);

---

[83] Article 3, Articles of Association, op. cit.

[84] Tiré du S.W.I.F.T. User Handbook, FIN Copy Service Description, Operations, November 1996.

[85] FIN Copy est effectué au sein d'un "closed group", Article 2.4. du FIN Copy Service Description, op. cit.

- Soit avant l'envoi à l'institution réceptrice (envoi en mode Y-Copy). Dans ce cas, c'est l'institution centrale qui autorise ou non l'envoi à l'institution réceptrice selon le contenu même du message, le solde des comptes des clients,....

## *Section 2 : Application de la directive*

FIN Copy n'étant qu'une variante du service de messagerie FIN ce sont les mêmes messages (ou une partie de ces mêmes messages) qui font l'objet du service et nous pouvons donc en conclure que des données à caractère personnel peuvent être contenues dans ceux-ci. De même, nous pouvons dire qu'il y a un "traitement" des données au sens de la directive puisque les données sont enregistrées, copiées et communiquées. La question est alors de déterminer si S.W.I.F.T. peut être qualifié de responsable du traitement.

Le responsable du traitement, nous le rappelons, est celui qui définit "les finalités et les moyens du traitement". Or puisque FIN Copy n'est qu'une variante du service FIN de S.W.I.F.T., il nous semble que les mêmes arguments que ceux développés précédemment peuvent être maintenus. D'une part, c'est l'institution qui envoie le message qui décide qu'il s'agit d'un message FIN Copy et que le message doit être envoyé à une institution tierce spécifiée. Dans ce cas le message sera alors automatiquement intercepté et envoyé à cette institution centrale. Elle décide donc de la finalité du traitement effectué[86]. Par ailleurs, elle peut déterminer quelles données sont à envoyer à l'institution mandatée. En effet, le message sera envoyé entièrement ou seulement en partie selon un accord préalable des parties. S.W.I.F.T. n'intervient pas dans la définition des finalités du traitement mais seulement en tant que moyen permettant la transmission du message. D'autre part, qualifier S.W.I.F.T. de responsable du traitement contribuerait à créer des risques nouveaux en lui accordant un "droit de regard" sur le contenu du message[87]. Pour ces mêmes raisons, nous estimons que S.W.I.F.T. ne peut être qualifié de responsable du traitement.

Pourtant, S.W.I.F.T. effectue un traitement "pour le compte" des utilisateurs, membres de S.W.I.F.T. . S.W.I.F.T. peut donc être qualifié de sous-traitant en ce qui concerne le service FIN Copy avec toutes les conséquences que cela comporte[88].

---

[86] Signalons que dans le cas d'un envoi en Y-Copy, l'institution centrale pourrait également être qualifiée de responsable du traitement dans la mesure où elle effectue son propre traitement sur les données afin d'accorder ou non l'autorisation d'envoi à l'institution finale.

[87] Pour plus de développements à ce sujet, voir *infra* Partie III, Chapitre III.

[88] Voir *supra* Partie II, chapitre I, section 1, 1D.

# CHAPITRE II : MESSAGE RETRIEVAL POLICY

## *Section 1 : Description du service*

Le Message Retrieval Policy est un service développé par S.W.I.F.T. afin de permettre à S.W.I.F.T. de retrouver des messages préalablement envoyés par le service de messagerie soit à la demande expresse des utilisateurs (émetteur ou destinataire du message), soit à des fins propres.

Dans le cas de demande de retrait des messages par un utilisateur, ce retrait se fait sur base d'un formulaire d'autorisation écrite (STP Authorisation Form) sur lequel l'institution requérante va définir les paramètres de recherche du retrait (tous les messages envoyés tel jour, tous les messages envoyés à telle banque ou vers tel pays,...). Dans le cas d'une procédure de recherche à des fins de statistiques c'est S.W.I.F.T. elle-même qui va définir les paramètres de recherche en fonction des statistiques à établir.

## *Section 2 : Application de la directive*

Il nous semble que ce service présente certaines particularités qui ne permettent plus de conclure à la qualification de S.W.I.F.T. comme simple sous-traitant. D'une part, les arguments tirés des considérants de la directive concernant le courrier électronique ou les services de télécommunications dont le seul objet est de transmettre des messages, ne sont plus soutenables dans cette hypothèse. S.W.I.F.T., dans le cadre du Message Retrieval Policy, fait plus que de transmettre purement et simplement des messages entre institutions. En effet, S.W.I.F.T. est obligé d'entrer dans le contenu même du message afin de retrouver les données définies dans les paramètres stipulés. Lorsque S.W.I.F.T. est chargé de retrouver tous les messages envoyés d'une institution A vers une institution B dont le montant est de plus de X million de francs, S.W.I.F.T. est obligatoirement amené à lire le contenu même du message, à l'analyser et à le soustraire ("retrieve") le cas échéant.

D'autre part, l'argumentation selon laquelle la qualification de S.W.I.F.T. comme responsable du traitement crée des risques supplémentaires de par le "droit de regard" qu'elle comporte, n'est plus soutenable puisque S.W.I.F.T. entre de toute façon dans le contenu même du message lorsqu'il fournit le service requis.

Enfin, la détermination du responsable du traitement se fait, nous l'avons vu, en fonction de la personne qui est, seul ou conjointement avec d'autres, à l'origine de la détermination "des finalités et des moyens du traitement de données à caractère personnel". Or dans le cadre de ce service, S.W.I.F.T. peut être à l'origine de la

détermination même de la finalité poursuivie. Il nous parait dès lors utile, à ce stade de notre réflexion, de faire une distinction selon les finalités poursuivies par le service[89].

### 1.A. Retrait à des fins propres

S.W.I.F.T. peut être à l'origine de la détermination même de la finalité poursuivie. Dans ce cas, selon le "Message Retrieval Policy", la finalité poursuivie est une finalité de statistiques afin de d'évaluer le service de messagerie offert par S.W.I.F.T. Le "message retrieval" peut porter uniquement sur des données relatives à l'utilisation du service ("raw traffic data") tels que par exemple le nombre de messages envoyés, la fréquence, la durée,... Dans ce cas le traitement ne porte pas sur des données à caractère personnel et la directive ne s'appliquera pas[90].

Le retrait et l'analyse peuvent également porter sur contenu même du message[91]: nombre d'envois pour un client déterminé, nombre d'envois portant sur une somme de plus de X millions,... Dans ce cas, si les données contenues dans le message concernent une personne physique identifiée ou identifiable, S.W.I.F.T. opère un traitement portant sur des données à caractère personnel pour lequel il sera qualifié de responsable du traitement. Selon nous, la seule manière pour S.W.I.F.T. de se décharger de cette qualification est de supprimer les données à caractère personnel contenues dans le message afin de ne plus tomber sous le coup de la directive.

### 1.B. Retrait pour des finalités définies par le requérant

Le message retrieval peut également se faire à la demande d'un requérant déterminé. Celui-ci peut être l'émetteur du message, le destinataire, ou le représentant d'un groupe d'utilisateurs[92]. La demande de retrait et d'analyse se fera soit sur des données relatives à l'utilisation du service, soit sur des données contenues dans le message en lui-même. Dans les deux cas, le champ d'analyse est déterminé par le requérant lui-même dans le STP Authorisation Form. L'analyse se fera soit par S.W.I.F.T., soit par un tiers auquel S.W.I.F.T. communiquera les données avec l'autorisation expresse du requérant. En cas de communication des données à un tiers, la détermination de la finalité poursuivie par le retrait et la communication du message se fait par le requérant lui-même. S.W.I.F.T. ainsi que le tiers à qui les données ont été

---

89 En principe la finalité du "retrieval disclosure policy" doit être préalablement déterminée dans un User handbook (voir Retrieval Data Policy)

90 Cela ne veut toutefois pas dire que S.W.I.F.T. n'encourt pas une certaine part de responsablilité en ce qui concerne la confidentialité de la relation entre ses clients, mais cela n'est pas un problème de protection des données à caractère personnel.

91 "Message data"

92 Dans ce cas S.W.I.F.T. devra contacter chaque membre du groupe afin de vérifier l'autorité du représentant.

communiquées ne peuvent utiliser les données pour d'autres finalités que celles qui ont été définies[93].

Une requête de retrait et d'analyse du message peut poursuivre plusieurs finalités distinctes: vérification de la bonne transmission du message, statistiques, évaluation de le rentabilité de certaines banques membres d'un groupe par l'autorité à la tête de celui-ci,.... Si la détermination de cette finalité se fait à priori par le requérant, il ne nous semble pas évident que S.W.I.F.T. n'ait aucun rôle à jouer. Il ne faut oublier, en effet, qu'en vertu de l'article 2 de la directive, la détermination de la finalité du traitement peut se faire par le responsable du traitement, "seul ou conjointement avec d'autres". Or ce service trouve sa place parmi les services offerts par S.W.I.F.T. en vertu de l'article 3.2. des Articles of Association, autorisant S.W.I.F.T. à créer ses propres services et produits pour autant que ceux-ci entrent dans le cadre du service de transmission initial. De plus, il apparait que les finalités poursuivies sont effectivement définies dans le "User Handbook" du service en question produit par S.W.I.F.T.

En tenant compte de ces considérations, tant que les messages traités dans le cadre de ce service contiennent des données à caractère personnel, il nous parait pas exclu que S.W.I.F.T.puissent être qualifié comme le responsable du traitement. Une solution envisageable afin d'échapper au champ d'application de la directive serait de retirer ou de masquer de manière définitive les données à caractère personnel contenues dans les messages.

## CHAPTER III : LES CONSÉQUENCES DE LA QUALIFICATION DE S.W.I.F.T. COMME RESPONSABLE DU TRAITEMENT

Puisque nous avons vu qu'il ne peut être exclu que S.W.I.F.T. soit qualifié de responsable du traitement dans les nouveaux services offerts, nous nous proposons d'analyser brièvement quelques unes des conséquences pratiques que cela pourrait impliquer pour S.W.I.F.T[94].

Les principes régissant la directive disposent que les données à caractère personnel ne pourront être "collectées que pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités". S.W.I.F.T. devra dès lors toujours déterminer la ou les finalités légitimes[95]

---

[93] "The requester must define the purpose of the disclosure of message data. The requester must also define the purpose of the disclosure of certain traffic data to be analysed. So neither S.W.I.F.T. nor the recipient are authorised to use the data for purposes other than those defined", Message Retrieval Policy, Draft rules and procedures, 4.viii.

[94] Si nous partons de l'idée que S.W.I.F.T. est une société établie en Belgique selon les termes de l'article 4.1. de la directive, la loi nationale belge prise en application de la directive sera d'application.

[95] La question de la légitimité de celles-ci dépendra dans une très large mesure de l'appréciation de la Commission de la Vie Privée.

poursuivies par le service offert. S.W.I.F.T. sera tenu également de notifier le traitement effectué auprès d'autorité nationale compétente (selon nous, il s'agira de la Commission de la Vie Privée belge dans la mesure où S.W.I.F.T. peut être considérée comme une société établie en Belgique).

Le traitement des données pourra uniquement se faire moyennant le respect des principes relatifs à la légitimation des traitements de données stipulés à l'article 7 de la directive. Si les données concernent un utilisateur du réseau, le traitement sera a priori permis dans la mesure où il est "nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci". Il existe, dans ce cas, un contrat entre S.W.I.F.T. et les utilisateurs du réseau, et le traitement est nécessaire pour l'accomplissement de celui-ci (message retrieval de données concernant les utilisateurs, personnes physiques, aux fins de vérifier la bonne transmission du message). Si, par contre, les données concernent une personne tierce à la relation entre S.W.I.F.T. et les utilisateurs du réseau (le client d'une banque, par exemple), l'on ne peut plus justifier le traitement de données personnelles concernant cette personne par le contrat existant entre S.W.I.F.T. et les utilisateurs. Le traitement, dans ce cas, pourra se fonder sur l'article 7.f de la directive dans la mesure où "il est nécesssaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou les tiers auxquels les données sont communiquées" (service offert par S.W.I.F.T. dans l'intérêt de son client et de la personne concernée (finalité d'assurer la bonne transmission des données) ou à des fins propres (dans le but d'établir des statistiques,...) et "à la condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée"[96]. A défaut de justification sur base de l'article 7.f, le traitement ne pourra se faire que moyennant le consentement indubitable de la personne concernée[97].

Quant à la qualité des données, celles-ci doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées ultérieurement. Par ailleurs, les données doivent être exactes et si nécessaires mises à jour. Il incombera dès lors à S.W.I.F.T. de veiller notamment à la qualité de données contenues dans le message lui-même, données relatives à des personnes avec lesquelles S.W.I.F.T. n'entretient bien souvent aucune relation déterminée (il peut s'agir, répétons le, de données relatives à des clients des utilisateurs du réseau). Enfin, les données ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une période

---

[96] Article 7.f de la directive. Il reviendra à la personne concernée d'apporter la preuve du déséquilibre entre les intérêts du responsable du traitement et de ses propres intérêts ou droits et libertés fondamentales.

[97] Nous imaginons les conséquences lourdes que cela implique pour S.W.I.F.T. qui, en principe n'est pas en relation directe avec ces personnes.

n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

Un niveau de sécurité approprié devra être mis en place par S.W.I.F.T. afin de protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. Puisque nous nous situons dans le cadre d'un réseau de transmission de données financières, il va sans dire que les risques présentés sont élevés (notamment d'accès non autorisé aux données) et que la nature des données est sensibles[98]. Remarquons que S.W.I.F.T. présente déjà un niveau de sécurité élevé dans ces services[99]. Il en va de la réussite même du réseau.

S.W.I.F.T. en tant que responsable du traitement sera tenu de remplir un certain nombre d'obligations à l'égard de la personne concernée par les données. Si l'idée au départ est de désigner un responsable unique vis à vis de la personne concernée, cela est parfois lourd de conséquences lorsque le responsable du traitement n'est pas en relation directe avec la personne en question. Ainsi, en vertu des articles 10 et 11 de la directive, S.W.I.F.T. sera tenu d'informer la personne concernée d'une série de renseignements afin de garantir un traitement loyal des données (sur son identité, la finalité du traitement, ...). Cette information se fera au moment même de la collecte, ou, si les données non pas été collectées directement auprès de la personne concernée, dès l'enregistrement de celles-ci ou de la première communication. Lors d'un message retrieval contentant des données personnelles relatives à un client d'un utilisateur pour une finalité déterminée par S.W.I.F.T. (statistiques, ...), S.W.I.F.T. devra informer cet utilisateur dès l'enregistrement de ces données pour cette finalité. En ce qui concerne l'information à fournir à un client d'un utlisateur, nous pourrions imaginer que cette information se fasse par le biais de l'utilisateur lui-même avec lequel le client entretient un contact direct.

Si qualifié comme responsable du traitement, S.W.I.F.T. devra également assurer à la personne concernée un droit d'accès à ses données et un droit de rectifier des données dont le traitement n'est pas conforme à la directive, notamment en raison du caractère incomplet ou inexact des données (article 12). Si la mise ne oeuvre de ce droit ne semble pas poser trop de difficultés en ce qui concerne les clients de S.W.I.F.T., et concernant des données auxquelles S.W.I.F.T. a d'office accès (données relatives à la transmission du message, par exemple), il n'en est sans doute pas de même en ce qui concerne les données contenues dans le message lui-même concernant des clients des

---

98 "Sensibles" non pas dans le sens donné par l'article 8 de la directive sur les catégories particulières de données, mais dans le sens que ces données concernent le profil financier d'un individu.

99 Voir Chapter 9 du FIN Service Description, op. cit.

utilisateurs. A ce propos, il est envisageable que le droit d'accès soit mise en oeuvre directement auprès de l'utilisateur avec lequel le client est en relation directe. S.W.I.F.T. est également tenu d'assurer un droit d'opposition au traitement de certaines données en cas de raisons prépondérantes et légitimes, et ne pourra prendre de décisions produisant des effets juridiques à l'égard de la personne concernée ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité[100].

Enfin, concernant les flux de données à caractère personnel vers des pays tiers à l'Union européenne, ces flux sont en principe interdits en ce qui concerne les pays qui n'assurent pas un niveau de protection adéquat (article 25). Toutefois, S.W.I.F.T. pourrait justifier un tel transfert sur base des exceptions prévues à l'article 25 de la directive et qui prévoit notamment que ce transfert est permis lorsqu'il est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée (transfert de données relatives aux utilisateurs du réseau). De même, un tel transfert est permis s'il est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure dans l'intérêt de la personne concernée, entre le responsable et un tiers (envoi de données concernant les clients des utilisateurs, par exemple). Dans les deux cas cités, il importe de vérifier la réelle nécessité du transfert des données par rapport au contrat. De plus S.W.I.F.T. pourrait être tenu d'informer la personne concernée que ses données sont envoyées vers un pays tiers n'assurant pas un niveau de protection adéquat aux yeux de la directive, dans la mesure où cette information est nécessaire pour assurer un traitement loyal des données à l'égard de la personne concernée (articles 10 et 11 de la directive).

## CONCLUSION

Si l'on peut conclure à l'applicabilité de la directive européenne relative à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel au réseau S.W.I.F.T., nous nous devons toutefois d'émettre une certaine réserve. En effet, il ne faut oublier que la directive ne donne que des principes généraux de protection des données, principes qui doivent être intégrées dans des dispositions nationales qui s'efforceront d'améliorer la protection assurée actuellement par leur législation et ceci dans les limites de la marge de manoeuvre accordée par la directive. En mettant en oeuvre la directive dans le droit national, les États membres restent donc

---

[100] S.W.I.F.T. aura une certaine facilité a effectuer ce type d'opérations dans la mesure où le service permet des recherches systématiques sur base des noms de clients. Des analyses de la fréquence d'utilisation du service, de types de transactions effectuées,....pourraient dès lors être à la base de décisions portant sur le profil de l'individu, sa rentabilité,...

libres d'interpréter les notions en cause voire de compléter les garanties offertes à la personne concernée. Une attention particulière devra dès lors être prêtée à la transposition de la directive dans la législation nationale par les différents États membres.

Une distinction doit être effectuée selon que l'on qualifie S.W.I.F.T. ou non de responsable du traitement :

Il nous semble que pour toutes les opérations dans le cadre des services FIN et FIN Copy, et portant sur des données contenues dans le message lui-même, S.W.I.F.T. ne peut être qualifié de responsable du traitement mais doit être considéré comme un sous-traitant, effectuant des opérations sur des données à caractère personnel pour le compte de ses clients. Cette qualification implique l'existence et le respect d'un contrat écrit entre S.W.I.F.T. et la personne qualifiée de responsable du traitement. S.W.I.F.T. ne pourra effectuer de traitements que sur instruction de ce responsable et ne pourra effectuer de traitement pour des fins propres. Par ailleurs, S.W.I.F.T. sera tenu de mettre en oeuvre des mesures de sécurité appropriées.

En ce qui concerne les données de transmission des messages (traffic data) de tous les services offerts par S.W.I.F.T., S.W.I.F.T. peut être qualifié de responsable du traitement. Cela n'impliquera, toutefois, un respect des dispositions contenues dans la directive, que dans la mesure où ces données sont relatives à des personnes physiques.

Enfin, nous estimons que S.W.I.F.T. peut être qualifié de responsable du traitement en ce qui concerne le service de Message Retrieval, dans la mesure où il effectue ce service pour des finalités propres. Il ne nous semble pas, toutefois, que cela soit lourd de conséquences pour S.W.I.F.T. En effet, Si cela implique une certaine limitation des finalités poursuivies , il ne nous semble pas que cela pose un problème pour les services offerts actuellement par S.W.I.F.T. qui trouveront un fondement légal dans l'article 7. En ce qui concerne le niveau de sécurité exigé, S.W.I.F.T. nous l'avons déjà dit, offre déjà à ses clients un niveau de sécurité élevé au sein de son réseau. Enfin, en ce qui concerne le respect et la mise en oeuvre de droits pour la personne concernée, soit S.W.I.F.T. se chargera du respect de ceux-ci auprès de ses clients utilisateurs du service (pour les données les concernant), soit il chargera ces derniers d'accomplir ces devoirs auprès de leurs propres clients avec lesquelles S.W.I.F.T. n'a en principe de contacts directs.