Europe et "privacy" : le cas swift. Analyse de l'applicabilité de la proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Boulanger, Marie-Helene; Léonard, Thierry; Poullet, Yves

Publication date:
1992

Document Version
le PDF de l'éditeur

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

EUROPE ET "PRIVACY": LE CAS SWIFT

ANALYSE DE L'APPLICABILITE DE LA PROPOSITION DE DIRECTIVE DU CONSEIL RELATIVE A LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

ETUDE REALISEE PAR
MARIE-HELENE BOULANGER
ET THIERRY LEONARD
SOUS LA DIRECTION
D'YVES POULLET

JUIN 1992

PLAN

INTRODUCTION

En 1990, la Commission des communautés européennes a émis une proposition de directive au conseil relative à la protection des personnes à l'égard du traitement automatisé de données. Ce texte pourrait avoir des répercussions significatives sur les activités menées par S.W.I.F.T. dans la mesure où celles-ci peuvent concerner de près ou de loin des données à caractère personnel, objet de la protection envisagée.

Dans une première partie, les concepts de base de cette proposition de directive seront envisagés d'une manière théorique. De la même façon, seront détaillés quelques principes fondamentaux de la directive particulièrement utiles dans le cadre de cette analyse. Le but à la base de cet exposé théorique est de poser le cadre de référence nécessaire à l'étude.

Dans une deuxième partie, plus concrète, les concepts et principes à la base de la directive seront confrontés au cas posé par le réseau S.W.I.F.T. La directive ayant été complétée par une directive sectorielle propre au secteur des télécommunications, celle-ci sera envisagée dans la mesure où elle peut contribuer utilement à l'analyse.

La troisième partie s'attachera à mettre en évidence les effets indirects que pourrait impliquer l'adoption du texte européen. De tels effets indirects se feraient sentir si les dispositions de la directive relatives aux flux transfrontières de données étaient appliquées aux membres utilisateurs du réseau. Enfin, en vue d'éviter ce risque, des pistes de solutions pratiques seront proposées.

PARTIE I : GENERALITES CONCERNANT LA PROPOSITION DE DIRECTIVE[1]

Il ne s'agira pas ici de passer en revue l'ensemble des dispositions contenues dans la Proposition de Directive mais bien d'introduire les notions indispensables pour résoudre la question de son applicabilité au réseau S.W.I.F.T.

---

1 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).

Le texte de la proposition faisant actuellement l'objet d'un examen approfondi, il est susceptible d'être largement modifié. Dès lors, il nous paraît utile de faire rapidement le point sur l'état de sa procédure d'élaboration.

Un premier texte, rédigé par la Commission, a été proposé par le Conseil. Celui-ci a suscité de nombreuses critiques au sein des milieux intéressés. Il a fait d'ores et déjà l'objet d'une relecture au sein du Conseil. Il a ensuite été examiné au Parlement. Ce dernier a approuvé une version amendée du texte[2]. A l'heure actuelle, il est impossible d'avoir une idée claire sur le contenu des dispositions définitives. Aussi, cet étude se base principalement sur la version originale du texte. Toutefois, il sera tenu compte de certaines modifications proposées si celles-ci présentent, d'après nos informations, de grandes chances d'être retenues ultérieurement. Quoiqu'il en soit, l'incertitude qui pèse sur l'avenir du texte rend particulièrement difficile l'adoption de conclusions définitives dans cette étude.

CHAPITRE I : OBJET DE LA PROPOSITION DE DIRECTIVE[3]

Sur le territoire de l'Europe communautaire les biens et marchandises, les capitaux, les services, les personnes circulent chaque jour plus librement. Sous-jacente et indispensable à ces mouvements, la libre circulation de l'information[4] s'est révélée être un complément incontournable des libertés fondamentales mises en place par le Traité de Rome[5], complément dont la réalisation est ressentie chaque jour davantage comme une nécessité[6].

Cependant, la libre-circulation des données au sein de la Communauté doit s'accompagner de la prise en compte scrupuleuse des libertés individuelles en jeu. C'est essentiellement la vie privée des individus qui est en cause. Cette notion doit être comprise dans son acception la plus large. Il ne s'agit pas, en effet, de vouloir préserver pour chacun un monde secret dont il a seul la clef, conception à laquelle la plupart opposent un "je n'ai rien à cacher, moi". Ce qui doit faire l'objet de la protection, c'est

---

2 Plus de 90 amendements au texte initial ont été proposés !

3 Cette section est largement inspirée d'un article écrit par Cécile de Terwangne et Marie-Hélène Boulanger sous la direction d'Yves Poullet commentant la proposition de directive. Celui-ci est actuellement en voie de publication.

4 Par "information", il faut entendre au sens de notre analyse toutes "données à caractère personnel", c'est-à-dire "toute(s) information(s) concernant une personne physique identifiée ou identifiable" (article 2a de la directive).

5 Article 8a du traité C.E.E.

6 2e et 4e considérants de la proposition de directive.

l'autonomie de l'individu, la maîtrise que celui-ci doit conserver de "l'image informationnelle" qui circule à son propos[7].

Ainsi que l'a fait remarquer le Parlement européen dès 1982, la Communauté se doit donc de "pallier les effets secondaires de ses activités (économiques et commerciales)"[8].

Si l'on veut toutefois voir la libre circulation des données réalisée et s'instaurer un véritable marché européen de l'information, il faut nécessairement viser à l'harmonisation des différents régimes nationaux.

Une première tentative de favoriser les flux d'informations mettant en cause des individus (données à caractère personnel) tout en assurant à ceux-ci la protection de leur image informationnelle, la maîtrise et le contrôle de l'information qui les concerne, a vu le jour sous l'égide du Conseil de l'Europe. Il s'agit de la Convention 108 de 1981[9]. Dix ans après le vote de ce texte, il faut toutefois constater avec regrets que la réalité n'a pas suivi les intentions. Une volonté d'harmonisation a peu à peu vu le jour. L'initiative en revint à la Commission européenne, qui a proposé en septembre 1990 un projet de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel[10].

Ce texte vise à traduire de façon plus précise les principes généraux contenus dans la Convention du Conseil de l'Europe afin de garantir une réelle équivalence des pratiques en matière de protection des données dans les pays membres et de permettre à ces derniers d'adopter une approche commune face aux pays tiers. La philosophie de la directive diffère de celle qui anime la Convention de 1981. En effet, alors que la Convention s'inscrit dans une perspective de protection des droits individuels, la directive est orientée vers une dynamique d'échange et de marché de l'information[11].

Le but avoué est d'éviter que les exigences de protection des données ne puissent entraver les mouvements transfrontières sur le territoire de la Communauté (article 1, paragraphe 2 de la directive). A l'inverse de la Convention 108 qui laisse une porte (légèrement)

---

7 C'est la Cour fédérale allemande qui, la première, tira de la protection constitutionnelle du droit à l'épanouissement de la personnalité , le "droit à l'autodétermination informationnelle".

8 Résolution du 5 mars 1982 relative à la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'information, J.O.C.E., n° C 87 du 5 avril 1982 , p. 30 Rapport Sieglerschmidt, doc.1-598/81.

9 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signée à Strasbourg, le 28 janvier 1981.

10 Document COM. (90) 314 final - SYN 287

11 V. 6e considérant de la proposition de directive : "... pour éliminer les obstacles à la circulation des données à caractère personnel le niveau de protection de la vie privée à l'égard des traitements de ces données doit être équivalent dans tous les Etats membres".

ouverte aux Etats parties pour faire obstacle au principe de libre circulation des données personnelles[12], la directive interdit formellement les restrictions entre Etats membres au nom de la protection des données.

Aucune des libertés mises en place au sein de la Communauté européenne n'est absolue. Toutes connaissent des exceptions, justifiées notamment par l'intérêt général[13]. La volonté présente derrière la directive est d'empêcher que chacun puisse à sa guise invoquer la protection de la "privacy" comme motif d'intérêt général pour mettre fin aux mouvements de l'information.

Il est toutefois à noter qu'un tel système présuppose l'existence d'un niveau équivalent de protection au sein de la Communauté. Or, l'article 28 de la directive envisage, en son deuxième paragraphe, que de "sérieuses divergences"[14] puissent être constatées entre la législation ou la pratique des Etats membres en matière de protection des données à caractère personnel. Cela semble donc contradictoire. Dans l'hypothèse où l'équivalence n'est pas acquise, un Etat se verrait-il en droit de freiner les échanges avec les pays moins protecteurs? Le principe de libre-circulation de l'information serait par là mis en péril.

En fait, la directive ne précise d'aucune manière ce que peut faire l'Etat qui constate une situation de sérieuse divergence. Il devrait dès lors être fait référence, dès l'article premier posant le principe de la liberté des flux (article 1.2), à l'éventualité de divergences dont fait écho l'article 28. Dans une telle situation, l'obligation de liberté tombe et l'Etat redevient juge de l'opportunité d'autoriser ou de prohiber l'échange des données. Mais cela affaiblirait d'emblée la position de la directive par l'aveu que l'harmonisation pourrait ne pas être réalisée.

---

12 L'article 12.3 de la Convention prévoit deux possibilités de dérogation au principe de liberté des flux : d'une part lorsque la législation d'un Etat prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données (données sensibles) ou de ces fichiers, et que la réglementation de l'autre Etat partie n'apporte pas de protection équivalente (12.3.a); d'autre part lorsqu'un transfert de données est projeté vers le territoire d'un autre Etat contractant, mais ce dernier pays ne servant que de lieu de transit vers un Etat tiers à la Convention, procédé qui permettrait de contourner la législation du pays d'origine (12.3.).

13 Cfr. articles 56 et 66 du Traité de Rome.

14 Le deuxième alinéa de l'article 28 stipule que "si le Groupe de protection des données à caractère personnel constate que de sérieuses divergences s'établissent entre la législation ou la pratique de Etats membres en matière de protection des données à caractère personnel, divergences qui risquent de porter atteinte à l'équivalence de la protection dans la Communauté, il en informe la Commission.

CHAPITRE II : DEFINITIONS ET CHAMP D'APPLICATION

Pour pouvoir appréhender l'impact de la directive en projet sur le réseau S.W.I.F.T. , il est indispensable de cerner avec précision le champ d'application territoriale envisagé ainsi que l'objet de la protection qui sera ainsi mise en place. A cette fin, dans une deuxième section nous envisagerons tout d'abord la portée de l'article 4 de la proposition de Directive (Section I). Quatre notions définies par le texte retiendront ensuite notre attention: les données à caractère personnel (Section II), le fichier (Section III), le traitement (Section IV) et le responsable du fichier (Section V).

Section I : Le champ d'application territoriale

L'article 4 a une double portée. D'une part, il désigne le domaine spatial d'application des règles de la future Directive transférées dans les ordres juridiques des Etats membres et ce, au moyen de critères précis de rattachement. D'autre part, il désigne indirectement la compétence de l'ordre juridique de l'Etat membre auquel la règle appartient.

Ainsi, la législation nationale d'un Etat membre contenant la transposition des principes de la directive s'appliquera :

1°) à tous les fichiers localisés sur son territoire;

2°) au responsable du fichier qui réside sur ce territoire et utilise depuis celui-ci un fichier localisé dans un pays tiers dont la législation n'a peut un niveau de protection adéquat, à moins que l'utilisation ne soit sporadique.

De plus, certaines dispositions, transposées dans les droits nationaux, devront s'appliquer à l'utilisateur qui consulte un fichier localisé dans un pays tiers à partir d'un terminal localisé sur le territoire d'un Etat membre, à moins que cette utilisation ne soit que sporadique.

Enfin, une disposition particulière vise les "déplacements temporaires" de fichiers d'un Etat membre à l'autre en prévoyant que ce dernier ne pouvait prescrire aucun obstacle ou formalité additionnelle aux règles applicables dans l'Etat membre de localisation permanente du fichier.

La principale difficulté de cet article provient des exceptions prévues en cas d'utilisation sporadique. Elles semblent avoir été motivées par la crainte que l'application de la

Directive n'entraîne des formalités trop lourdes. On a donc souhaité ne pas y soumettre des utilisateurs occasionnels d'autant que les risques d'atteinte à la vie privée paraissent être plus faibles dans ce cas, tout du moins du point de vue quantitatif.

Cela étant, on peut se demander si le critère de la fréquence d'utilisation du fichier, auquel renvoie le terme sporadique, est bien approprié. En effet, il n'y a pas de corrélation nécessaire entre la fréquence d'utilisation du fichier et le risque d'atteinte présenté par l'utilisation.

Une dernière remarque concerne le concept de localisation du fichier sur le territoire d'un Etat membre. Comment apporter une preuve certaine de la localisation d'un fichier à un endroit précis alors que les nouvelles technologies offrent aux données une mobilité extrême?

Section II : Les données à caractère personnel

Afin de circonscrire le champ d'application de la proposition de Directive, il nous faut préciser la notion de "données à caractère personnel"[15], concept-clef de la protection communautaire.

La définition retenue par la proposition de directive est quasi-identique à celle adoptée lors de l'élaboration de la Convention n°108 du Conseil de l'Europe, définition par ailleurs présente en termes similaires dans de nombreuses législations nationales. Entre donc dans le champ de la directive "toute information concernant une personne physique identifiée ou identifiable"[16]. Le texte poursuit en apportant des précisions sur ce qu'il faut entendre par personne identifiable. Bien que l'illustration soit donnée en des termes peu ouverts ("personne qui peut être identifiée par référence à un numéro d'identification ou une information similaire"), on peut considérer que toute méthode d'identification doit être prise en compte.

En toute logique, tout ce qui n'est pas donnée à caractère personnel est donnée anonyme et par ce fait, se retrouve hors du champ de la directive. La définition de l'"anonymisation" permet ainsi de circonscrire par l'extérieur la notion de donnée personnelle.

Au sens de la directive, la donnée anonyme est celle qui ne peut plus être reliée à une personne physique déterminée ou déterminable, "ou moyennant seulement un effort

---

15 On trouve aussi, principalement dans les textes législatifs et la pratique française, la notion de "données nominatives".

16 Article 2.a. de la proposition de directive.

excessif en personnes, en frais et en temps"[17]. Tant que les efforts consentis pour identifier un individu auquel rattacher des données ne sont pas excessifs, les données seront donc considérées comme "à caractère personnel", l'individu étant identifiable[18].

La référence à un effort excessif soulève de nombreuses réactions au sein des milieux concernés. Elle prend cependant en compte le fait que les données ne sont pas anonymes une fois pour toutes mais peuvent éventuellement être repersonnalisées. Toutefois, le caractère excessif est relatif et doit s'apprécier en fonction des moyens dont dispose le détenteur des données. Ainsi des données qui seraient anonymes pour une administration qui ne dispose pas des moyens techniques ou financiers de les rattacher à des individus (efforts excessifs), pourraient donc être librement transférées à une entreprise. Or, pour celle-ci, les efforts à fournir ne seront peut-être pas excessifs au vu de l'importance de ses moyens. Les données, anonymes au départ, doivent être alors de nouveau couvertes par la protection.

Section III : Le fichier

Le champ d'application de la directive est défini par référence à la notion de "fichier"[19] : "les Etats membres appliquent les dispositions de la présente directive aux fichiers du secteur privé et du secteur public à l'exclusion des fichiers du secteur public dont les activités ne relèvent pas du champ d'application du droit communautaire".

Le maintien de la notion de fichier -dépassée pour d'aucuns- est totalement pertinent d'un point de vue formel, dans la mesure où il offre une base matérielle pour les formalités administratives. Utilisée généralement à bon escient dans la directive, cette notion recouvre l'objet d'un certain nombre de procédures administratives (notification du fichier, déclaration du fichier, ...) qui poseraient des problèmes de praticabilité si elles devaient être effectuées sur la base des traitements[20].

Une innovation intéressante à souligner est la prise en considération de la réalité des réseaux informatiques "qui permettent aux données de se disperser tout en pouvant être reliées à volonté à travers la possibilité d'un dialogue d'ordinateur à ordinateur ou de

---

17 Article 2.b. de la proposition de directive.

18 Cela conforte donc notre large interprétation de la notion d'individu "identifiable".

19 Par "fichier" il faut entendre, aux termes du projet de directive "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.).

20 Voy. projet de loi belge qui exige la déclaration de tout traitement (projet de loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, ch., sess. ord., 90-91, 6 mai 1991, 1610/1).

terminal à ordinateur"[21]. C'est dans ce sens qu'il faut comprendre la définition du fichier visant des données "centralisées ou réparties sur plusieurs sites".

Notons ici qu'à l'exemple de la majorité des législations européennes en vigueur ou en voie de le devenir, les auteurs du projet de directive entendent soumettre les fichiers manuels aux règles protectrices.

Aux termes des définitions présentes dans la proposition de Directive, le fichier représente les données à caractère personnel faisant l'objet de traitements et détenues par le maître du fichier. Ces deux derniers concepts, vu l'objet de ce travail, demandent un approfondissement.

Section IV : Le traitement

L'article 2. d de la proposition de directive du Conseil définit le traitement comme "les opérations, effectuées ou non à l'aide de procédés automatisés : enregistrement, conservation, interconnexion de données, leur modification, leur utilisation et leur communication, notamment la transmission, la diffusion, l'extraction, ainsi que le verrouillage, l'effacement et la destruction".

En termes simples, on peut dire que le traitement consiste, d'après ce texte, en une ou plusieurs utilisation(s) particulière(s) d'un ensemble de données à caractère personnel. Il peut consister en différentes opérations définies plus ou moins largement selon la réglementation en cause (voir infra).

Il suppose une unité fonctionnelle[22] qui va souder entre elles ces différentes opérations portant sur les données. C'est l'ensemble des moyens mis en oeuvre pour faire concourir des données à une finalité choisie qui constitue un traitement particulier.

On remarque dès lors que structurellement, le traitement est indissociable de la notion de finalité. On ne peut perdre cette caractéristique de vue.

La proposition définit de manière exhaustive les types d'opérations tombant sous son champ d'application. De sorte que l'on peut dire qu'à partir du moment où les données

---

21 X., *Les nouvelles technologies : un défi pour la protection de la vie privée ?*, Conseil de l'Europe, Strasbourg, 1989, p.35.

22 Concernant le traitement automatisé, voir CNIL, ` *rapport d'activités-1978-1980*, Doc. Fr., Paris, 1980, p.25.

sont collectées, toute utilisation[23] de celles-ci fait partie intégrante d'un traitement susceptible d'être réglementé. Cette définition est remarquablement étendue, ce qui est une bonne chose. Elle pourra être appliquée à un maximum de situations susceptibles de mettre en danger les droits de la personne dont les données sont traitées.

Section V : Le responsable du fichier

En l'état actuel du texte, la proposition de directive définit le responsable du fichier comme : "La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon le droit communautaire ou la loi nationale d'un Etat membre, pour décider quelle sera la finalité du fichier, quelles catégories de données à caractère personnel doivent être enregistrées, quelles opérations leur seront appliquées et quels sont les tiers qui peuvent y avoir accès".

D'après l'exposé des motifs[24], les rédacteurs ont clairement voulu préciser ici que celui qui autorise la consultation, notamment en cas d'interrogation directe, est le responsable du fichier. Cette notion est capitale puisque la proposition de Directive y rattache directement de nombreuses obligations[25] faisant du responsable du fichier le garant de la protection. Ainsi est-il non seulement responsable de la sécurité des données (article 18) mais d'une manière générale de tout dommage qui serait subi par les personnes concernées par les données "du fait du traitement ou de toute action incompatible avec les dispositions de la présente Directive"[26].

Sa responsabilité risque en outre de se voir engagée lorsqu'il charge un tiers de traiter des données à caractère personnel pour son compte (article 22). Dans ce cas, il s'agira cependant d'une responsabilité partagée, le tiers restant soumis aux obligations prévues à l'article 18 (sécurité des données) et à l'article 16 (qualité des données). Le but recherché est d'éviter que ce cas de figure ait pour conséquence l'affaiblissement de la protection de la personne concernée[27]. La référence à l'article 16 est cependant fortement remise en cause par certains pays membres[28]. Ceux-ci estiment en effet qu'en ce qui concernent les sous-traitant, la responsabilité contractuelle suffirait à assurer la protection de l'individu. Le responsable du fichier mis en cause peut, en cas de violation de la privacy, se retourner contre l'agent à qui il a confié le traitement sur base du contrat qui les lie. Ce serait donc au responsable de fichier de prévoir les dispositions de protection de la vie

---

23 Au sens large du terme, "'utilisation" des données est d'ailleurs reprise comme telle dans la liste des opérations.

24 Exposé des motifs, COM (90) 314 final SYN 287 (13 septembre 1990), p. 21.

25 Voir par exemple articles 6.3, 8.2, 9.1, 11.1 etc...

26 Article 21.1.

27 Exposé des motifs, COM (90) 314 final SYN 287 (13 septembre 1990), p. 44.

28 Notamment l'Allemagne, le Danemark, les Pays-Bas et le Royaume-Uni.

privée dans le contrat conclu avec le tiers à qui il confie le traitement de données à caractère personnel.

CHAPITRE III : COMMUNICATION DES DONNEES

La directive est assez permissive quant aux conditions sous lesquelles les données personnelles peuvent être communiquées. Ainsi, la communication est en principe libre, pour autant qu'elle ne soit pas incompatible avec la finalité du fichier (c'est au ficheur qu'il revient de prouver la compatibilité) et qu'elle ne porte pas atteinte à l'ordre public.

La notion de "communication" n'est pas définie dans le texte de la directive. Communément entendu, ce terme vise la transmission des données à un tiers. Dans la mesure où la communication met donc en cause la notion-clef de "tiers", c'est en fait cette dernière notion qui demande à être précisée.

Par "tiers", on peut entend toute personne qui n'est pas sous l'autorité du responsable du fichier. Dans le cas de personnes morales, l'analyse de l'organisation juridique de ces personnes, critère clair et fiable, devrait permettre de déterminer si celui qui demande communication des données est soumis à l'autorité du responsable du fichier. Il y aurait dès lors communication lorsque des données sont transmises à un tiers, même si celui-ci est situé à l'intérieur de l'entreprise du maître du fichier. Par contre, il n'y aurait pas communication si le destinataire des données est un établissement géographiquement distinct mais sous l'autorité du même responsable. Bien sûr, il n'est pas question de considérer qu'il y a lieu à communication quand le tiers auquel les données sont transmises est la personne concernée par les données elle-même ou celle qui traite les données pour le compte du maître du fichier (service-bureau).

CHAPITRE IV : FLUX TRANSFRONTIERES DE DONNEES

L'examen de la problématique des flux transfrontières de données à destination de pays tiers à la communauté européenne nous paraît devoir être envisagé lors de l'analyse de l'applicabilité de la directive européenne "privacy" au cas de S.W.I.F.T. En effet, d'une part, S.W.I.F.T. dans la mesure où il pourrait être considéré comme responsable d'un fichier devrait respecter les dispositions applicables en la matière. D'autre part, même si S.W.I.F.T. ne peut être englobé sous cette qualification, les membres européens affiliés au réseau peuvent quant à eux clairement être qualifiés de responsables de fichiers de données à caractère personnel. Dès lors, dans la mesure où ils envoient des messages

financiers vers des pays tiers, ils devront prendre en compte les principes régissant les flux transfrontières ce qui pourrait avoir un impact sur l'activité même de S.W.I.F.T. (voir infra).

Examinons à présent le régime envisagé. La proposition de directive réglemente de manière spécifique les flux transfrontières de données à destination de pays tiers à la Communauté européenne. Elle érige en principe, l'interdiction de tout transfert de données vers les Etats tiers qui n' assurent pas à celles-ci un niveau de protection adéquat (Section I). Le texte prévoit cependant certaines dérogations à ce principe de base (Section II).

La volonté du législateur -tant national que communautaire- d'assujettir les données à une réglementation limitant leurs possibilités d'exportation vise généralement à éviter que les mesures de protection instaurées au sein d'un Etat ne soient affaiblies par des traitements effectués dans un pays tiers dont la législation plus libérale favoriserait la création d'un "paradis de données"[29]. Concrètement, le péril naîtrait d'une liberté absolue reconnue aux responsables de fichiers ressortissant de la Communauté européenne d'exporter les données à caractère personnel vers des Etats tiers, une liberté qui pourrait bien les conduire à "délocaliser" leurs fichiers en vue de les soustraire aux dispositions contraignantes de la directive.

Fidèle à la logique de son projet, le législateur communautaire entend pallier au mieux son impuissance face aux autorités nationales étrangères qui échappent à son contrôle pour des raisons évidentes tenant à la souveraineté étatique. Cette action préventive se traduit dans la proposition de directive par une stricte réglementation de l'exportation des données personnelles. Il requiert en effet, en son article 24, al. 1, que les législateurs nationaux érigent en principe que le transfert temporaire ou définitif de données faisant l'objet d'un traitement ou collectées en vue d'un traitement ne peut avoir lieu que pour autant que le pays importateur leur assure un niveau de protection "adéquat".

Section I : Principes de base (article 24).

La procédure mise en place par la proposition de directive étant relativement élaborée, il nous paraît utile d'en reprendre les différentes étapes.

L'article 24 §1 dispose que les Etats membres incluront dans leur législation une disposition interdisant le transfert de données vers des Etats ne leur assurant pas un niveau de protection adéquat. Il reviendra dans un premier temps aux Etats membres

---

29 voy. sur cette question F. Rigaux, "Le régime des données informatisées en droit international privé", Journal de droit international, 1986, pp. 311-328.

d'établir le caractère adéquat ou non de la protection accordée aux données par le pays tiers importateur. Ceux-ci devront évaluer le niveau de protection assuré par les pays tiers vers lesquels des exportations ont lieu. Le texte ne précise pas les moyens devant être utilisés à cet effet. Les Etats membres sont donc libres de choisir le système qui leur semble le plus approprié. Cependant, il apparaît en toute logique qu'au sein de chaque Etat membre, le pouvoir décisionnel reviendra à l'autorité de protection de données puisque celle-ci sera amenée à connaître des communications de données et notamment de celles destinées à l'étranger [30].

Si l'Etat membre estime la protection adéquate, il devrait normalement avaliser le transfert. A l'opposé, s'il estime que la protection offerte par le pays tiers n'est pas adéquate, il bloquera le transfert et en informera la Commission[31] .

C'est sur base de ces informations fournies par les Etats membres, ou éventuellement à partir d'autres renseignements, que la Commission sera amenée à constater que le pays en question ne dispose pas d'un niveau de protection adéquat. Elle pourra alors entamer des négociations en vue de remédier à la situation. Le troisième paragraphe de l'article 24 pose une condition préalable à l'amorce de négociations : la situation doit être préjudiciable que ce soit aux intérêts de la Communauté ou d'un Etat membre. Le texte ne précise cependant pas si les négociations doivent être menées avec le pays tiers ou avec l'Etat membre ou au choix avec l'un ou l'autre ou encore les deux selon le cas. L'exposé des motifs ne mentionnant que des négociations entre la Commission et le pays tiers concerné, on peut penser que c'est cette situation que le texte a voulu rencontrer.

Ajoutons que l'information communiquée par l'Etat membre à la Commission devra être répercutée auprès des autres Etats membres en vue de suspendre tout transfert similaire de données à partir d'un autre pays de la CEE (voir infra).

Le quatrième paragraphe de l'article 24 précise ensuite que la Commission pourra décider qu'un pays tiers offre bien une protection adéquate. Pour ce faire, elle prendra l'avis du comité consultatif et fondera son appréciation sur les deux critères suivants : l'état de la législation interne et l'existence d'engagements internationaux souscrits par l'Etat en question.

Certains commentaires spécifiques peuvent être émis en ce qui concerne la portée du concept "adéquat" .

---

30 Voy. art. 6.3 du projet de directive en ce qui concerne les traitements du secteur public et 11.1 pour ceux du secteur privé.

31 Article 24 al.2 de la proposition de directive

L'évaluation du caractère adéquat de la protection présentée par un pays tiers risque de se révéler particulièrement délicate. La notion même de protection "adéquate" était inconnue jusqu'ici. La Convention du Conseil de l'Europe avait retenu, pour sa part, une approche s'appuyant sur le concept de protection équivalente. Ainsi, tout en érigeant en principe la libre circulation des données, la Convention admet que des restrictions[32] puissent être apportées en l'absence de protection équivalente dans le chef du pays tiers importateur de données[33]. La détermination de critères d'appréciation de ce dernier concept a déjà donné lieu à de nombreuses discussions et controverses[34]. D'aucuns se sont notamment demandé si l'équivalence de la protection offerte devait être évaluée de façon globale à l'égard d'un pays déterminé ou s'il fallait l'évaluer au cas par cas en fonction du flux particulier posant problème.

A première vue, la notion de protection adéquate semble, quant à elle, faire référence à une exigence de protection moindre. Le texte du projet de directive ne fournit que peu d'indications relatives aux critères de décision : l'appréciation du caractère adéquat pourra en particulier se fonder sur les engagements internationaux souscrits par le pays tiers importateur de données ou sur base de la législation nationale de ce dernier.

Le premier critère repose sur l'adhésion du pays importateur à des normes internationales. A la lumière d'un premier tour d'horizon, seule la ratification de la Convention du Conseil de l'Europe[35] nous apparaît comme constitutive d'une preuve suffisante en soi, mais peut-il en être de même de la simple adhésion aux lignes directrices du Conseil de l'OCDE[36] ?

Le second critère repose sur l'évaluation de la législation nationale. La difficulté qu'a suscité l'interprétation du concept de protection équivalente se retrouve ici. Deux interprétations procédant de démarches différentes sont envisageables. D'une part, une telle évaluation peut procéder d'une appréciation globale de la réglementation du pays destinataire des données ou d'autre part de la volonté de retrouver la trace des principes de base de la proposition de directive dans le droit national du pays soumis à l'appréciation.

---

32 - Voy. les articles 3 (2) (a), 12 (3) (a).

33 Les législations française, allemande, hollandaise et anglaise contiennent également des dispositions permettant de restreindre le libre-échange d'informations.

34 voy. L. Early, "Securing equivalent protection among nations in the context of transborder data flow : a possible role for contract law (the standard contract proposed bythe Council of Europe", Droit de l'informatique et des télécoms, 1990, 4, pp. 10-14.

35 L'exposé des motifs reprend explicitement la convention du Conseil de l'Europe à titre d'exemple des engagements que la Commission prendra en compte.

36 La ratification de la Convention du Conseil de l'Europe implique que le pays en question ait adopté une législation nationale et donc que les deux critères d'appréciation formulés dans le texte du projet soient réunis.

Si nous nous référons à la première possibilité, à savoir l'appréciation globale de la réglementation du pays destinataire des données, l'interprétation que donneront les Etats membres et la Commission du caractère adéquat de la protection mise en oeuvre par le pays tiers court le risque d'être particulièrement laxiste en raison d'impératifs politiques et économiques. Pratiquement, nous nous imaginons difficilement que l'un ou l'autre Etat membre ou la Commission estime de manière globale que la législation d'un pays comme les Etats-Unis n'offre pas un niveau de protection adéquat. Ce dernier Etat, pourtant, privilégie une approche sectorielle[37].

Le paradoxe de ce dernier constat illustre l'intérêt d'une autre approche. Ainsi, la notion de protection "adéquate" peut également être comprise comme se référant à l'existence dans un pays tiers d'une protection des données qui reprenne les principes de base de la proposition de directive. Le système mis en oeuvre par le pays tiers aboutirait à une protection similaire à celle instaurée dans la Communauté, bien que les moyens utilisés à cet effet diffèrent sensiblement. La protection établie pourrait prendre diverses formes : sans revêtir nécessairement l'aspect d'une loi générale de protection des données, elle pourrait par exemple être constituée de réglementations spécifiques à un secteur[38], voire même être assurée par le biais de codes de bonne conduite. L'approche communautaire s'apparenterait donc, selon cette évaluation, plutôt à une approche sectorielle de la notion de protection adéquate. Cette démarche, tout empreinte de pragmatisme, nous paraît devoir être retenue car elle permet une appréciation plus fine et plus nuancée et, par là-même, favorise la mise en oeuvre de la disposition. Il ne s'agit en effet pas de condamner de manière globale la politique adoptée par un pays en matière de protection des données mais plutôt d'apprécier la protection offerte par cet Etat dans un secteur déterminé.

Notons encore à cet égard que la notion de protection adéquate prête le flanc à une appréciation toute subjective. Si nous nous référons au sens usuel du terme adéquat, nous apprenons qu'il signifie approprié, ajusté à son but. La protection requise ne serait-elle donc point susceptible de vérification objective ?

Rappelons à ce stade qu'un pays ne pourra en principe transférer des données à caractère personnel vers un pays tiers que si ce dernier qui leur assure un niveau de protection adéquat[39]. L'article 25 du projet de directive adoucit toutefois quelque peu la rigidité de ce principe d'interdiction.

---

37 Les fichiers privés font l'objet de règles particulières généralement applicables à un secteur professionnel déterminé, voy. par exemple, le Fair Credit Reporting Act (1970) (Public Law, n° 91.508, 15 U.S.C. §§ 1681-1681t) amendant le Consumer Credit Protection Act.

38 "EC launches data protection initiative", T.D.R., oct. 1990, p. 6.

39 L'Etat exportateur disposera normalement d'une législation nationale de protection des données conforme à la directive.

Section II : Dérogations (article 25)

L'Etat membre hôte du fichier peut autoriser le transfert "sur présentation par le responsable du fichier de justifications suffisantes pour garantir le respect d'un niveau de protection adéquat"[40]. Il ne s'agit pas à proprement parler de l'application extra-territoriale de la directive mais bien de l'obligation à charge de l'exportateur européen, d'assurer par des moyens adéquats la protection de la vie privée lorsque les données sont traitées à l'étranger.

Pour ce faire, l'article 25 prévoit une procédure d'information de la Commission et des Etats membres assorti d'un délai de notification d'opposition de 10 jours. En cas de notification d'opposition, la Commission pourrait prendre les mesures appropriées et notamment, aux termes de l'exposé des motifs, décider d'interdire le transfert[41].

La question qui surgit d'emblée est de déterminer si l'inclusion de clauses contractuelles d'adhésion aux principes de protection des données dans le contrat conclu entre l'exportateur et l'importateur de données suffira à assurer aux données une protection suffisante.

Nous ne pouvons en effet passer sous silence l'inconvénient majeur propre au recours au recours aux clauses contractuelles de garantie, à savoir l'absence à la cause de l'individu fiché. Ce dernier, dont nous ne pouvons nier l'intérêt pour ces questions, n'étant pas partie au contrat passé entre le fournisseur et le destinataire des données, ne pourra faire valoir aucun droit ni introduire de recours dans l'hypothèse d'une utilisation erronée ou abusive des données. Aucune solution certaine ne permet à l'heure actuelle de remédier à cet état de choses. Mais le contrat devrait en tout état de cause inclure une clause assurant un droit d'accès et de correction dans le chef de l'individu concerné par les données.

Une seconde difficulté apparaît alors. Pour que les individus fichés jouissent d'une protection réellement efficace, il est important de leur offrir des possibilités de recours

---

40 Le recours à des clauses contractuelles -reprenant les principes de protection des données de la Convention du Conseil de l'Europe et de la loi française du 6 janvier 1978 et notamment reconnaissant des droits d'accès et de rectification aux personnes concernées- avait déjà été imposé par la CNIL française dans l'affaire FIAT. Il s'agissait en l'espèce de transmission d'informations relatives aux cadres supérieurs entre FIAT France et FIAT Italie ; délibération n° 89-78 du 11 juillet 1989 relative à la transmission d'informations relatives aux cadres supérieurs de la société FIAT France à la société FIAT à Turin. La CNIL a fait application des mêmes principes dans d'autres affaires (informatisation du Centre de Sécurité Sociale des Travailleurs Migrants, délibération n° 89-98 du 26 septembre 1989 : Eurocode)

41 La Commission est tenue de prendre l'avis du Comité consultatif selon la procédure prévue à l'article 30 §2.

s'inscrivant dans le cadre la législation "privacy" de leur pays en cas d'utilisation abusive des données à l'étranger[42]. Comment assurer aux autorités chargées de la protection des données un réel pouvoir hors des limites géographiques de leur compétence rationae loci [43]? Seule la mise en place d'une procédure de contrôle a priori du contenu des données exportées nous paraît pouvoir contourner cette difficulté.

Enfin, l'adoption d'une exception supplémentaire autorisant le transfert vers un pays ne garantissant pas un niveau de protection adéquat basée sur le consentement de l'individu doit-elle être envisagée ? Reconnaître telle exception permettrait de transférer des données personnelles dans le cas ou cela s'avère indispensable à la fourniture d'un service à la personne concernée. Ainsi concrètement, le transfert de données consécutif à une transaction internationale, vers un pays dépourvu d'un niveau de protection adéquat serait autorisé pour autant que la personne concernée y consente. Ce consentement se devrait d'être informé au sens où il est entendu dans la proposition de directive[44], l'information devant centrée plus spécifiquement sur la non-existence d'un niveau de protection adéquat et le risque dès lors encouru. De plus, les informations ainsi transmises ne devraient pouvoir être utilisées qu'aux seules fins de fourniture du service.

La justification de pareille exception résiderait dans l'intérêt légitime de la personne concernée de décider elle-même de ses besoins personnels. Le transfert se ferait donc dans l'intérêt de la personne concernée souhaitant obtenir un service nécessitant de manière impérative un transfert de données personnelles.

Le consentement comme exception au principe d'interdiction d'exportation vers un pays n'offrant pas de niveau de protection adéquat ne devrait avoir lieu que dans le cadre d'une relation contractuelle ou quasi-contractuelle. Admettre une telle exception rencontrerait les objections de certains commentateurs inquiets de ne pouvoir effectuer des paiements internationaux. Les deux conditions cumulatives, suffisantes à leurs yeux à assurer la protection de l'individu, seraient donc d'une part le consentement informé de la personne concernée au transfert et d'autre part que le transfert ait lieu dans le cadre d'une relation contractuelle et qu'il soit nécessaire pour l'exécution d'une obligation contractuelle.

---

42 B.W. Napier, "Contractual solutions to the problem of equivalent data protection in transborder data flow, op. cit., p. 33; voy. également A. Bourlond, "Le recours aux clauses contractuelles pour assurer la protection des données à caractère personnel dans le cadre des flux transfrontières" (en voie de plublication).

43 voir A.C.M. Nutger, Transborder Data Flow of Personal Data within the EEC, Utrecht, Kluwer, 1990, p.309.

44 Article 12 de la proposition de directive.

CHAPITRE V : OBLIGATIONS DU RESPONSABLE DU FICHIER

Cette partie a pour but de passer succintement en revue les obligations qui, dans l'état actuel du texte[45], devront être prévues dans les législations de chaque Etat membre à charge des responsables de fichiers qui tombent sous leur champ d'application.

Section I : La légitimité du traitement

Dans le secteur privé, la légitimité du traitement est fondée sur le consentement de la personne concernée (art. 8.1). Si ce dernier n'est pas obtenu, le projet prévoit que l'enregistrement ou le traitement des données à caractère personnel ne sont légitimes qu'en accord avec les dispositions de la Directive et si :

a. soit le traitement se situe dans le cadre d'un contrat ou d'une relation de confiance quasi-contractuelle avec la personne concernée tout en étant nécessaire à sa réalisation;

b. soit les données proviennent de sources généralement accessibles au public et leur traitement est uniquement destiné à des fins de prospect commercial ou publicitaire;

c. soit le responsable du fichier poursuit un intérêt légitime à condition que l'intérêt de la personne concernée ne prévale pas.

Les Etats membre pourront préciser les conditions de légitimité du traitement (art. 8. 3).

Quant au consentement, il doit être exprimé en conformité avec les dispositions des articles 12 relatif au consentement informé et 13 relatif à l'information lors de la collecte.

Il ne faut pas non plus oublier que la personne concernée peut toujours s'opposer, pour des raisons légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (art. 14. 1).

---

45 92 amendements ont été adoptés par le Parlement européen. Nombreux sont ceux qui seraient susceptibles de modifier les obligations du maître du fichier. Il est malheureusement impossible de savoir aujourd'hui ceux qui ont le plus de chance d'être retenus dans la version définitive du texte final. Ce qui sera dit dans cette partie est donc à prendre avec "réserve". Il n'empêche que cela donnera au lecteur une idée du type d'obligation qui pèse généralement sur le maître du fichier dans les législations "privacy".

Enfin, le responsable du fichier devra s'assurer que toute communication des données n'est pas incompatible avec la finalité du fichier et qu'elle ne porte pas atteinte à l'ordre public (art. 8. 3).

Section II : Le traitement des données sensibles

Sauf accord libre, exprès et écrit de la personne concernée, le responsable du fichier ne peut traiter des données révélant l'origine raciale et ethnique, l'opinion politique, les convictions religieuses ou philosophiques, les appartenances syndicales ainsi que les informations relatives à la santé et à la vie sexuelle de la personne concernée (art. 17. 1).

Des dérogations peuvent être prévues au sein des législations nationales aux conditions fixées par l'article 17. 2.

Les données concernant des condamnations pénales ne peuvent être conservées que dans des fichiers relevant du secteur public (art. 17. 3).

Section III : La collecte des données

L'article 16 a) du projet pose le principe selon lequel la collecte des données à caractère personnel doit être effectuée loyalement et licitement. Pour rendre ce principe effectif, l'article 13 prévoit que les personnes auprès desquelles les données sont collectées se voient octroyer le droit d'être informé au-moins sur :

1° les finalités du fichier auquel les informations sont destinées et

2° le caractère obligatoire ou non de leur réponse aux questions qui font l'objet de la collecte et

3° les conséquences à leur égard d'un défaut de réponse et

4° les destinataires des informations et

5° l'existence du droit d'accès et de rectification des données le concernant et

6° le nom et l'adresse du responsable du fichier.

Ces informations permettront à la personne concernée d'être attentive aux risques éventuels d'atteintes à sa vie privée qui pourraient être engrengés par le traitement. Elles lui donnent également les renseignements nécessaires afin de contrôler l'utilisation des données.

Section IV : Le respect du principe de finalité

Les responsables de fichier ne peuvent enregistrer des données à caractère personnel que pour des finalités déterminées, explicites et légitimes.

La finalité sera déterminée au sens de la proposition si le but de l'enregistrement et de l'utilisation des données est défini et spécifié de façon aussi précise que possible Une définition ou une description générale ou vague de l'objet d'un fichier (par exemple "à des fins commerciales") est donc proscrite. Cette finalité est à spécifier soit avant l'enregistrement soit, le cas échéant, avant la collecte des données[46]

Le caractère explicite de la finalité oblige le responsable du fichier à divulguer celle-ci afin d'éviter que les traitements soient effectuées dans des buts cachés[47].

La légitimité des finalités met en exergue le fait que les finalités potentielles d'un fichier sont limitées. Les buts doivent être compatibles avec les dispositions de la proposition de directive et celles des législations nationales des Etats membres. Dans le secteur privé, les finalités correspondent au domaine d'activités commerciales des responsables de fichiers[48].

Ces données doivent en outre être utilisées de manière compatible avec ces finalités (art. 16. 1. b). C'est pourquoi le responsable ne peut traiter que des des données adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées.

Section V : L'information de la personne concernée

Deux cas de figure doivent être distinguées. Soit le responsable du fichier conserve les données à caractères personnel soit il se propose de les communiquer.

Dans le premier cas, le projet ne prévoit pas explicitement une information de la personne concernée. Cependant, l'article 14. 3 enjoint aux Etats membres de lui octroyer le droit de connaître l'existence du fichier, ses finalités principales ainsi que l'identité et la résidence habituelle, le siège ou l'établissement du responsable du fichier.

---

46 Exposé des motifs, COM (90) 314 final SYN 287 (13 septembre 1990), p. 37.
47 Idem.
48 Idem.

Dans les législations nationales, l'effectivité de ce droit sera vraisemblablement rendue possible par deux moyens différents:

1° obliger le responsable du fichier qui traite les données à procurer lui-même l'information à la personne concernée[49] et/ou

2° prévoir un registre au niveau national accessible au public et reprenant les informations relatives aux maîtres du fichier[50].

Généralement, ses deux possibilités seront prévues cumulativement.

Dans le second cas, l'article 9 de la proposition impose que le responsable informe la personne concernée de la première communication des données ou de l'ouverture d'une possibilité de consultation en ligne et indique également la finalité du fichier, les types de données qui y figurent, et ses noms et adresses.

Grâce à ces informations, la personne concernée pourra exercer son droit d'accès et, le cas échéant, s'opposer au traitement. Le responsable est alors tenu de cesser le traitement contesté, sauf si une disposition légale l'y autorise.

Notons que des exceptions sont prévues notamment lorsque la communication est imposée par la loi (art. 9. 2).

Par ailleurs, les Etats membres auront la possibilité de prévoir des exceptions au principe d'information pour autant que l'on soit dans les conditions fixées par l'article 10.

Section VI : L'accès aux données

Les personnes concernées se voient reconnaître le droit d'obtenir à des intervalles raisonnables la confirmation de l'existence ou non dans un fichier de données à caractère personnel le concernant et ce, sans délais ou frais excessifs. Le cas échéant, le responsable du fichier les lui communiquera sous une forme intelligible (art. 14. 4).

---

49 Voir l'article 10 du projet de loi belge (Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.*, Ch., sess. ord. 1990-1991, n°1610/1, p. 75.

50 Voir l'article 19 du projet de loi belge (*Op. cit.*)

Section VII : La correction, la remise à jour des données et leur répercussion

Les données doivent être exactes et, si nécessaire, mises à jour. Les données inexactes ou incomplètes devront être effacées ou rectifiées (art. 16. 1. d- 14.5).

Le responsable du fichier doit aussi notifier la rectification aux tiers qui ont obtenu la communication des données corrigées (art. 14. 7).

Section VIII : La limitation de la durée de conservation et l'effacement ou le verrouillage des données

L'article 16 1. e prévoit que les données ne doivent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée qui n'excède pas celle nécessaire aux finalités pour lesquelles elles ont été enregistrées.

Lorsque le traitement n'est pas conforme aux dispositions de la directive, la personne concernée à le droit de demander au responsable du fichier leur effacement ou leur verrouillage (art. 14. 5).

Ceux-ci devront être notifiés aux tiers à qui les données ont été communiquées (art. 14. 7).

Section IX : La notification à l'autorité de contrôle

Si les données sont destinées à être communiquées et qu'elles ne proviennent pas de sources généralement accessibles au public, le responsable notifie l'établissement du fichier qui les contient auprès de l'autorité de contrôle compétente. Il lui transmettra également tout changement d'adresse ou de finalité du fichier (art. 11. 1).

Il reviendra aux Etats membres de définir quelles informations feront l'objet de cette notification. Elles doivent comprendre au-moins le nom et l'adresse du responsable du fichier, la finalité du fichier, une description des types de données qu'il contient, les tiers auxquels les données sont susceptibles d'être communiquées et une description des mesures de sécurité qui ont été prises (art. 11. 2).

Section X : La sécurité et les flux transfrontières

Nous renvoyons ici aux développements apportés supra.

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

Dans quelle mesure le réseau S.W.I.F.T. est-il susceptible d'être compris dans le champ d'application de la proposition de Directive ? Tel est l'objet de la présente partie.

Remarquons de prime abord que cette étude se centre sur les 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 préoccuperons 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, l'application de la future Directive ne fait aucun doute.

Avant d'entrer dans le vif du sujet, il paraît intéressant de montrer l'analogie pouvant être faite entre le réseau S.W.I.F.T. et ce que l'on appelle communément les systèmes de "courrier électronique".

Selon une définition largement admise[51], ce dernier système consiste en un terminal et un clavier, capables de transmettre des messages codés par l'intermédiaire du réseau téléphonique auquel le ou les destinataires sont reliés. D'autres services peuvent y être inclus dont la boîte aux lettres électronique où le destinataire trouve les messages enregistrés et envoyés.

Il semble bien que l'on puisse soutenir que le réseau S.W.I.F.T. réponde largement à cette définition. En effet, l'utilisateur y trouve un moyen efficace d'envoyer des messages financiers aux autres participants d'un réseau de télécommunication géré par la société S.W.I.F.T. Ce réseau est constitué de terminaux reliés entre eux par des lignes de transmissions de données 'haute vitesse' louées auprès de sociétés de téléphone privées ou publiques. Le fait que le transporteur soit une entreprise privée et non un service public ne modifie en rien la nature du service proposé.

Cette remarque préliminaire est importante pour la suite du raisonnement. En effet, dès le milieu des années 80, le Conseil de l'Europe s'est interrogé sur la pertinence de l'approche qu'il avait adoptée lors de la mise en oeuvre de la Convention n°108 pour la

---

51 CONSEIL DE L'EUROPE, *Les nouvelles technologies : un défi pour la protection de la vie privée ?*, Strasbourg, 1989, p.29.

protection des données[52]. Il est parti du constat suivant lequel ce texte reflétait un état de la technologie des années septante largement dépassé quelques années plus tard.

Il a mis sur pied un groupe de travail chargé de réfléchir sur la capacité des concepts existants [53] à appréhender les problèmes spécifiques des technologies de l'information les plus récentes. Une des technologies envisagées était le courrier électronique. La réflexion menée a débouché sur un rapport[54] qui présente une grande utilité pour cette analyse[55]. Cependant, les particularités du réseau S.W.I.F.T. ainsi que l'objet spécifique de la recherche - l'applicabilité de la proposition de Directive du Conseil et non de la Convention n°108 - amènent à des conclusions originales qui s'écartent quelque peu de celles émises par le Conseil de l'Europe en matière de courrier électronique.

Cette partie sera divisée en deux grands chapitres correspondant à la distinction qui doit être opérée entre d'une part les données à caractère personnel contenues dans les messages et d'autre part celles générées par l'utilisation du réseau.

CHAPITRE I : LES DONNÉES CONTENUES DANS LES MESSAGES

Section I : Définitions

A. Données à caractère personnel

Après une analyse des messages S.W.I.F.T., il apparaît clairement que certains de ceux-ci contiennent des données à caractère personnel au sens de l'article 2a de la proposition de directive. En effet, ils reprennent dans certains cas le nom de personne(s) physique(s) auxquelles on peut associer la teneur du message. Le message "MT 100" (Customer Transfer) en est un bon exemple.

---

52 Convention n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Série des Traités européens*, Janvier 1981, n°108.

53 Les concepts de la Convention 108 se retrouvent d'ailleurs dans les réglementations nationales, la Convention ayant été insérées dans les législations des parties contractantes.

54 CONSEIL DE L'EUROPE, *Les nouvelles technologies : un défi pour la protection de la vie privée?*, Affaires juridiques, Strasbourg, 1989.

55 Il est certain que la référence au travaux du Conseil de l'Europe donne un poids particulier aux raisonnements tenus dans cette étude.

Reprenons en l'adaptant le cas de la page 4.7. du user handbook[56]. Franz Holsapfel[57] demande à la Oesterreichische Laenderbank (Vienna) de transférer 1,958.47 florins à l'Algemene Bank Nederland Amsterdam au bénéfice de H.F. Jansen.

Le message S.W.I.F.T. se présente de la façon suivante :

Explanation	Format
Sender	OELBATWW
Message Type	100
Receiver	ABNANL2A
Message Text	
Transaction Reference Number	:20:494931/DEV
Value Date/Currency Code/Amount	:32A:910527NLG1958,47
Ordering Customer	:50:FRANZ HOLZAPFEL VIENNA
Beneficiary Customer	:59:H.F. JANSSEN LEDEBOERSTRAAT 27 AMSTERDAM
End of Message Text/Trailer	

H.F. Jansen et Franz Holsapfel sont bien des personnes physiques identifiables. Le nom de chacun apparaît en toutes lettres dans le message. A ce nom sont rattachées différentes informations notamment la banque où il ont un compte, le montant de la transaction, le type de monnaie dans laquelle elle se fait et en ce qui concerne Jansen son adresse. Bien entendu, la prise de connaissance des données implique le décryptage du message en cause. Le cryptage n'équivaut cependant pas à une anonymisation des données. La lecture du message n'implique pas pour S.W.I.F.T. un effort excessif en personnel, en frais et en temps au sens de l'article 2b de la proposition de directive.

La même analyse est valable pour d'autres types de messages tels : le MT 110 (advice of cheque : p. 14-7), le MT 111 (request for stop Payement of a cheque : p. 15-5), le MT 810 (p.14-9 du livre concernant les travellers cheques) mais aussi le MT 192, le MT 292 et le MT 455 etc.

B. Traitement

Pour qu'il y ait "traitement", certaines opérations doivent être effectuées sur des données à caractère personnel à l'aide de procédés automatisés ou non.

Le réseau S.W.I.F.T., réseau privé international pour la télécommunication financière, se charge de l'envoi de messages via un système électronique de transmission. On accède à

---

56 Standards-2 Payments Cash management Customer Status, version 1.4 91/3 p. 4.7.

57 Pour les besoins de l'analyse, nous avons fait abstraction du fait que Franz Holsapfel soit constitué en société.

celui-ci par un terminal d'ordinateur. On peut donc dire sans doute possible que les messages contenant des données à caractère personnel sont communiqués par des procédés automatisés au sens de l'article 2d de la proposition de directive.

Les opérations à la base du traitement tel que défini par le texte de la proposition sont notamment l'enregistrement, la conservation, l'utilisation, la communication et l'effacement des données à caractère personnel. Il est à remarquer que la définition du traitement sera très vraisemblablement amendée en vue d'inclure parmi ces opérations la collecte des données[58]. Pour qu'il y ait traitement, il n'est pas nécessaire que l'ensemble des opérations soit effectué, il suffit que l'une et/ou l'autre soit mise en oeuvre dans un but déterminé[59].

L'enregistrement et la communication des données à caractère personnel sont inhérents à la fonction première du réseau S.W.I.F.T. : l'envoi de messages financiers. Certains de ceux-ci, on l'a vu, nécessitent l'enregistrement de données à caractère personnel. Le transfert du message implique leur communication. Ces opérations d'enregistrement et de communication ne sont pas effectuées pour elles-mêmes mais s'avèrent indispensables à la réalisation du service proposé.

En outre, le bon fonctionnement du réseau implique le stockage des messages. Les données à caractère personnel contenues dans ces derniers font donc l'objet d'une conservation. Cette conservation a lieu pour deux finalités distinctes. D'une part, il s'agit de garantir au transfert des messages une fiabilité maximale. Ainsi, les messages seront archivés au niveau des Slice Processors. D'autre part, il est nécessaire de conserver des moyens de preuve en cas de contestation portant sur la réalité ou sur le contenu des messages. Ainsi, les utilisateurs peuvent en obtenir une copie en ligne durant une période de 14 jours. Passé ce délai, celle-ci pourra être obtenue sur demande écrite adressée au "Chief Inspector Officer" puis, par courrier, pendant quatre mois. La conservation s'inscrit d'ailleurs dans une procédure spécifique d'arbitrage des conflits entre utilisateurs du réseau[60].

On pourrait donc dire que S.W.I.F.T. opère indirectement certains traitements sur des données à caractère personnel via les messages dans lesquels celles-ci sont contenues.

---

58 Amendement proposé par le Parlement européen (n° 179 Hoon).

59 Voir par exemple Paris (9ème Ch.), 31 mai 1991, *Expertises*, n°148, Mars 1992, pp.117 & svtes et note J. FRAYSSINET.

60 M. ANTOINE, J.-F..BRAKELAND, M. ELOY, *Le droit de la preuve face aux nouvelles technologies de l'information*, Bruxelles, Story-Scientia, 1992.

C. Fichiers

La notion de fichier telle que définie par la proposition de directive vise tout ensemble de données à caractère personnel centralisées ou réparties sur plusieurs sites faisant l'objet d'un traitement automatisé.

On l'a vu, des données à caractère personnel sont présentes dans le système et font indirectement l'objet de traitements. La question sera ici de déterminer si les messages conservés dans le système pour les finalités précédemment décrites représentent des fichiers au sens de la proposition de Directive.

Les conséquences d'une possible disparition de la notion de fichier dans le futur texte de la directive seront ensuite rapidement passées en revue.

Le rassemblement et la conservation des données à caractère personnel via les messages dont elles font partie intégrante ne nous paraissent pas constitutifs de fichiers au sens de la proposition de Directive.

L'exposé des motifs précise clairement que la définition du fichier est fondée sur le critère de la possibilité d'accès aux données à caractère personnel. Les risques d'atteinte à la vie privée apparaissent principalement lorsqu'un regroupement des données disséminées peut être effectué.

En insistant sur le fait que les données peuvent tout aussi bien être centralisées que réparties sur plusieurs sites[61], la proposition de Directive rencontre les critiques émises relativement à l'inadéquation de la notion de fichier au sens de la Convention n°108 du Conseil de l'Europe et des législations nationales dérivées face à l'émergence de réseaux informatiques[62]. La réalité visée ici est celle de données dispersées pouvant être reliées à volonté entre elles à travers un dialogue d'ordinateur à ordinateur ou de terminal à ordinateur. Ce phénomène est typique d'une organisation fonctionnant selon le schéma suivant : un réseau local et différentes personnes qui extraient et traitent des données à caractère personnel à partir de différents points d'accès au réseau. En redéfinissant le concept de fichier, la proposition de Directive vise ainsi à prendre en considération les risques d'atteintes à la vie privée découlant de l'éventuelle émergence au niveau du réseau d'un "fichier logique" composé de données géographiquement dispersées mais pouvant

---

61 Ce qui n'était pas le cas dans la Convention n°108.

62 CONSEIL DE L'EUROPE, *Les nouvelles technologies : un défi pour la protection de la vie privée?*, Affaires juridiques, Strasbourg, 1989, p.35 et 36.

être rassemblées par le biais de manipulations informatiques. Le fichier logique permettrait donc "de situer en dernier ressort, à travers des méthodes d'extraction, toutes les données dispersées dans le réseau à la suite d'un traitement et d'un enregistrement légitimes au sein d'une organisation donnée"[63].

Le réseau S.W.I.F.T. est bien un réseau informatique au sens des considérations précitées. Toutefois, cela ne nous paraît pas impliquer qu'il génère un fichier au sens de la proposition de Directive.

C'est ici qu'il convient de mettre en évidence les particularités du réseau S.W.I.F.T. pouvant comme nous l'avons vu, être assimilé à un système très perfectionné de "courrier électronique".

Toutes proportions gardées, le service offert par S.W.I.F.T est comparable à un service postal. Le message financier est confié au réseau électronique tout comme la lettre au réseau traditionnel de transmission du courrier. Personne ne soutiendra que la poste est responsable d'un gigantesque fichier manuel alimenté par les données contenues dans les lettres qu'elle transmet. Il est remarquable que dans ces hypothèses, les deux institutions ne prennent pas connaissance des données elles-mêmes mais procèdent seulement à un contrôle formel des messages qui les contiennent. Dans le cas du réseau S.W.I.F.T., les messages remplacent les lettres mais le but des deux institutions est identique. Dans les deux cas, la dispersion des données à caractère personnel est telle que le rassemblement et la conservation des messages qui les contiennent ne peuvent établir l'existence d'un ensemble de données à caractère personnel au sens de l'article 2.c de la proposition de Directive.

Cette constatation découle de l'absence complète de structure[64] du "rassemblement" de données à caractère personnel découlant du stockage des messages. Aucun lien n'est établi entre les données à caractère personnel contenues dans les différents messages.

Certes, S.W.I.F.T. dispose, dans l'absolu, de possibilités particulières offertes par l'informatique et l'automatisation lui permettant d'extraire aisément des données personnelles et de les utiliser dans d'autres buts que leur simple communication. Force est de reconnaître que cette potentialité ne s'est pas concrétisée à ce jour.

Comme les données à caractère personnel n'apparaissent qu'au fur et à mesure de la réalisation de l'objet même de la société, à savoir, le transfert de messages financiers, on

---

63 *Idem*, p.36.

64 Pour un raisonnement analogue voir CONSEIL DE L'EUROPE, *Les nouvelles technologies : un défi pour la protection de la vie privée?*, Affaires juridiques, Strasbourg, 1989, p.36.

est a priori assez éloigné des banques de données, bases de données ou autres fichiers traditionnels principalement visés par les législations privacy. Ce qui explique notamment la difficulté d'appréhender le réseau S.W.I.F.T. sur base des concepts traditionnels de la privacy.

Enfin, il est à noter que les messages ne sont conservés que durant une période assez courte à savoir le temps nécessaire à garantir la preuve du contenu du message en cas de contestation. Cette conservation limitée nous paraît également aller contre l'idée de rapprochement entre les données.

L'ensemble de ces considérations nous amène à conclure que les données à caractère personnel contenues dans les messages ne présentent pas les caractéristiques suffisantes pour être analysées comme se retrouvant dans des fichiers au sens de l'article 2.c de la proposition de Directive.

En l'état actuel du texte de la proposition de directive, la notion de fichier reste un des éléments fondamentaux du système de protection. Cette notion est cependant remise en question par le Parlement européen qui a voté un amendement[65] visant à le supprimer purement et simplement du texte définitif.

Il semble bien que cette modification ait peu de chances d'être reprise par la Commission. Toutefois, dans un souci d'exactitude et de précision, cette éventualité doit être prise en compte dans ce travail.

Si la notion de "fichier" disparaissait, la protection se baserait alors sur le concept de "données à caractère personnel". Le réseau S.W.I.F.T. utilisant de telles données, pourrait-on conclure à l'application de la proposition de Directive ? La réponse nous paraît négative car même dans ce cas, S.W.I.F.T. ne pourrait sans doute pas être considéré comme le "responsable des données", cette dernière notion devant être comprise dans un sens quasi-identique de celui de "responsable du fichier".

D. Responsable du fichier

Le responsable du fichier est celui qui organise le fichier, décide des principes de gestion et de l'utilisation qui en sera faite. Ainsi, il déterminera quelles sont ces finalités, quelles données seront enregistrées et quelles opérations peuvent être appliquées à celles-ci. Il lui appartiendra encore de décider des tiers qui peuvent y avoir accès.

---

65 Amendement n° 14 du Parlement européen, Procès-verbal de la séance du mercredi 11 mars 1992, 1992-1993, doc. PE 160.503.

S.W.I.F.T. organise-t-il un fichier de données à caractère personnel en vue de finalités propres qu'il détermine lui-même ?

La réponse doit être négative dès l'instant où l'on admet que S.W.I.F.T. ne détient aucun fichier[66] (voir supra). Cette société ne saurait organiser un fichier qui n'existe pas, c'est évident. Nous développerons toutefois une réflexion particulière sur ce point car des caractéristiques propres à la notion de responsable du fichier s'opposent également à ce que S.W.I.F.T. puisse être considéré comme tel. Cette approche se justifie également du point de vue de la logique d'argumentation puisqu'elle permet de faire face à un éventuel refus de notre théorie concernant l'absence de fichier.

Si nous refusons le qualificatif de "responsable du fichier" à la société S.W.I.F.T. c'est d'abord parce qu'aucune finalité particulière n'est donnée aux renseignements à caractère personnel contenus dans les messages. Certes, S.W.I.F.T. décide de la structure des messages. La standardisation de ceux-ci est en effet une nécessité absolue. Elle a permis l'harmonisation d'une multitude de pratiques, conventions et usages régissant antérieurement le transfert des messages financiers. L'automatisation des échanges est à ce prix. L'apport de S.W.I.F.T. consiste donc dans la formalisation et la rationalisation de l'échange d'informations financières.

Il en est tout autrement en ce qui concerne le contenu même des messages. Celui-ci est totalement dépendant des pratiques habituelles des affaires. Le succès de S.W.I.F.T. en dépend! Cette affirmation n'est pas uniquement théorique, la standardisation des messages se fait avec la participation active des utilisateurs du réseau. Des groupes de travail ad hoc sont mis sur pied pour "address international financial business functions" et pour s'assurer que les standards S.W.I.F.T. sont compatibles avec les pratiques commerciales en vigueur. Ils sont notamment chargés de développer de nouveaux standards de messages[67]. Ceci illustre à souhait que la présence de données à caractère personnel dans des messages n'est pas recherchée en soi, mais répond à des besoins découlant de la nature même des messages. On ne peut donc dire que S.W.I.F.T. décide effectivement des catégories de données à caractère personnel qui doivent être enregistrées.

Dans le même ordre d'idées, S.W.I.F.T ne décide pas d'opérations spécifiques effectuées sur les données à caractère personnel contenues dans les messages. Elle n'opère que sur le message peu importe qu'il contienne ou non des données à caractère personnel.

---

66 CONSEIL DE L'EUROPE, *Op. Cit.*, p.37.

67 User handbook, version 1.1 91/2, p. 2.2.

S.W.I.F.T. n'intervenant que pour transférer des messages entre utilisateurs qui lui en font la demande, il est évident qu'il ne décide nullement des tiers pouvant accéder aux données.

Pour toutes ces raisons, il nous paraît raisonnable d'affirmer que S.W.I.F.T. ne peut être considéré comme responsable d'un fichier au sens de la proposition de Directive européenne et ce, en ce qui concerne les données à caractère personnel contenues dans les messages.

Cela peut être admis en ce qui concerne l'activité principale de S.W.I.F.T. Toutefois, dans la mesure où S.W.I.F.T. utiliserait les données à caractère personnel dans un but différent du transfert des messages au sens strict, il serait susceptible d'être considéré comme responsable du fichier.

Une situation risque bien d'être interprétée en ce sens. On a vu qu'une procédure particulière a été mise sur pied au sein de la société afin d'arbitrer les conflits entre membres portant sur les messages qu'ils s'envoient. Les messages et par conséquent les données qu'ils contiennent sont stockés par S.W.I.F.T. qui jouera le rôle d'arbitre en cas de désaccord entre les utilisateurs du réseau. La finalité du stockage est donc particulière. Le service ainsi rendu, bien que présentant un lien certain avec l'activité principale de transmission, consiste en une utilisation spécifique des messages. Il faut souligner une fois de plus que cette finalité particulière ne porte pas sur les données en tant que telles mais a trait aux messages objet de l'échange. Les remarques qui ont été faites sur ce point peuvent donc être réitérées.

Remarquons encore que si cette procédure infère un traitement direct sur les données à caractère personnel, elle n'implique nullement un rapprochement ni une utilisation spécifique de celles-ci. La contestation porte sur l'une ou l'autre rubrique d'un message en particulier. Le but de la procédure sera alors de vérifier le message afin d'y corriger une rubrique erronée (le montant indiqué par exemple). Loin de constituer une atteinte abusive aux droits de la personne concernée, le traitement participe à un but parfaitement légitime qui sert ses avantages : la recherche de la vérité. Évidemment, ceci ne suffit pas à justifier la non-application des règles nationales protectrices. Toute critiquable qu'elle soit, cette application conduirait à de larges dérogations fondées tant sur le but du traitement et le faible risque d'atteinte à la vie privée qu'il engendre [68].

---

68 S.W.I.F.T. pourrait par exemple bénéficier de règles particulières relativement à l'obligation de déclaration à l'autorité nationale de contrôle (voir article 18 §7 du projet de loi belge).

Enfin, il ne fait aucun doute que S.W.I.F.T. puisse être qualifié de responsable du fichier s'il acceptait de fournir sur demande des renseignements concernant les personnes physiques apparaissant dans les messages. Tel serait par exemple le cas où un service de police exigerait de S.W.I.F.T. qu'il coopère à une enquête et communique les ordres de paiement émis par une personne soupçonnée de blanchir l'argent ou d'effectuer des transferts vers des paradis fiscaux.

Cela étant, même si S.W.I.F.T. n'échappe pas totalement à l'application du texte de la proposition de Directive même lorsqu'il ne peut être considérée comme responsable du fichier. En effet, diverses obligations sont mises à charge de ceux qui traitent des données à caractère personnel pour le compte du responsable du fichier.

Section II : Un traitement pour compte des responsables de fichiers

A. Notion

Le texte actuel ne définit pas de manière explicite ce qu'il faut entendre par "traitement pour compte du responsable du fichier". Les débats suscités par cet article montrent que la situation visée est celle où une personne - le responsable du fichier - confie en sous-traitance à une autre - l'agent traitant - le soin de mettre en oeuvre un traitement. Ce dernier doit être entendu au sens large comme incluant la collecte des données (art. 22.2).

L'agent traitant est donc un tiers par rapport à la relation entre le maître du fichier et la personne concernée par le traitement des données. Il est là pour effectuer une tâche particulière sur les données, étant entendu qu'une fois celle-ci réalisée, il n'utilisera ni les données de base, ni les résultats du traitement qui reviennent de droit au responsable du fichier.

La protection de l'individu concerné est garantie normalement par les obligations grevant le responsable du fichier dans la mesure où il effectue lui-même le traitement. S'il le confie en tout ou partie à un tiers, il n'est plus en mesure d'exercer directement son contrôle. Des garanties particulières doivent donc être prévues.

C'est l'objet de l'article 22 de la proposition de Directive qui met sur pied un système de responsabilité partagée entre le maître du fichier et l'agent traitant.

Ainsi, en ce qui concerne le responsable du fichier, les législations des Etats-membres doivent prévoir qu'il assure le respect des mesures nécessaires de sécurité et

d'organisation. Il est également tenu de choisir une personne ou une entreprise qui apporte des garanties suffisantes à cet égard.

L'agent traitant, quant à lui, devra respecter les obligations prévues aux articles 16 et 18 de la proposition de Directive.

L'article 16 concerne la qualité des données. Si l'agent traitant collecte et traite des données pour le compte du responsable du fichier, il devra respecter le principe de loyauté et de licéité. Le traitement effectué devra aussi se conformer aux finalités légitimes déterminées par le responsable du fichier. Il devra en outre veiller à ce que les données soient adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles ont été enregistrées. De plus, celles-ci doivent être exactes et mises à jour. L'agent traitant se chargera donc, le cas échéant, de les rectifier. Enfin, il doit être attentif à ce que les données soient effacées au cas où la durée de conservation excéderait celle nécessaire à la réalisation des finalités pour lesquelles elles ont été enregistrées.

L'article 18 concerne la sécurité des données. Le but ici est double. D'une part, éviter que la vie privée de la personne concernée ne soit mise en péril soit par le responsable du fichier dans le cadre de son activité soit en cas d'utilisation abusive des données par des tiers qui, sans autorisation, accèdent aux données[69]. L'agent sera donc tenu de "prendre les mesures techniques et d'organisation appropriées et nécessaires à la protection du fichier contre la destruction, accidentelle ou non autorisée, la perte accidentelle, ainsi que contre l'altération ou l'accès et tout autre traitement non autorisé de données à caractère personnel".

L'exposé des motifs précise que ces mesures "comprennent celles relatives à l'accès aux locaux de traitement et de conservation des données, des codes d'identification pour les personnes autorisées à se rendre dans ces locaux et des garanties réelles que l'utilisation de mots de passe pour l'accès à des fichiers informatisés, le cryptage de données, et la surveillance du piratage et d'autres activités inhabituelles. En ce qui concerne les mesures d'organisation, le responsable du fichier doit adopter certaines procédures au sein de la hiérarchie de son administration ou de son entreprise, par exemple en établissant des niveaux d'autorité pour l'accès aux données"[70].

Ces mesures permettront à l'agent d'"assurer pour les fichiers automatisés un niveau de sécurité approprié compte tenu, d'une part, de l'état de l'art en la matière et du coût de leur mise en oeuvre et, d'autre part, de la nature des données à protéger et de l'évaluation des risques potentiels".

---

69 Exposé des motifs, COM (90) 314 final SYN 287 (13 septembre 1990), p. 40.

70 Exposé des motifs, COM (90) 314 final SYN 287 (13 septembre 1990), p. 41.

Cette dernière obligation semble particulièrement vague. Il semble bien que la Commission n'ait pas voulu imposer un niveau très élevé de sécurité afin d'éviter de grever les petites entreprises de charges trop élevées. Il n'empêche que l'adéquation des mesures à l'état de l'art en la matière et aux coûts supportés pour leur mise en oeuvre risque bien de poser des problèmes d'interprétation considérables.

L'article 18.2 impose également à l'agent traitant de choisir des méthodes garantissant une sécurité adéquate pour la transmission des données à caractère personnel dans un réseau. Nous verrons que cette obligation semble aller à l'encontre de la qualification de S.W.I.F.T. comme agent traitant.

Le point 3 de l'article 18 prévoit les mesures de sécurité devant être prises au cas où le responsable du fichier permettrait à un tiers d'accéder aux données traitées par l'agent.

Le point 4 rappelle que les trois premiers points sont applicables aux personnes qui ont, de fait ou par contrat, le contrôle des opérations relatives au fichier. Cette mention est surabondante en ce qui concerne l'agent traitant puisque l'article 22.2 dit clairement que l'article 18 lui est applicable. Toutefois, 18.4 vise des situations plus larges que celui de l'agent traitant, ce qui lui rend toute son utilité.

Le dernier point de l'article 18 impose en outre que toute personne qui accède aux informations contenues dans des fichiers et ce, dans le cadre de ses activités professionnelles, ne les communique pas à des tiers sans l'accord du responsable du fichier. Cette obligation doit-elle être respectée par l'agent traitant ? A priori, une hésitation est permise puisque le point 4 l'obligeait seulement au respect des trois premiers points. La réponse paraît cependant positive car l'article 22 ne fait aucune distinction de cette sorte en prévoyant le respect des obligations prévues à l'article 18.

Enfin, l'article 22.3 édicte qu'un contrat doit être dressé entre le responsable du fichier et l'agent traitant. Celui-ci doit être écrit et spécifier, en particulier, que les données à caractère personnel ne peuvent être divulguées par l'agent ou son personnel qu'avec l'accord du responsable du fichier.

Force est finalement de constater que l'article 22 ne délimite pas clairement les responsabilités du responsable du fichier et de l'agent traitant. S'ils sont tous les deux soumis aux articles 18 et 16, il n'est pas précisé qu'ils sont tenus solidairement responsables en cas de non-respect de ces dispositions. On ne peut dès lors qu'espérer une clarification lors de la transposition du principe dans les différentes législations nationales.

Nul ne peut dire non plus si cet article restera rédigé de cette manière. La référence à l'article 16 a donné lieu à de nombreuses critiques de la part des différents pays membres. Certains pensent en effet que le partage de responsabilité ne se justifie qu'au niveau du contrôle et non en ce qui concerne la qualité des données. Pour se protéger lorsqu'il n'est pas en mesure de garantir personnellement le respect de l'article 16 de la future Directive, le responsable du fichier pourrait d'ailleurs obtenir de son cocontractant qu'il s'engage à le respecter dans une clause ad hoc insérée dans le contrat.

B. Application

La question qui se pose à nous est de savoir si S.W.I.F.T. peut être considéré comme agent traitant des données à caractère personnel pour le compte des responsables de fichier, in casu, les utilisateurs du réseau.

Les données à caractère personnel qui transitent par le réseau S.W.I.F.T. proviennent des fichiers des différents utilisateurs. Afin de réaliser certaines opérations financières pour le compte de leurs clients, ceux-ci doivent transmettre certaines données les concernant. Cette communication est une opération particulière effectuée sur les données dans une finalité spécifique. Il pourrait donc s'agir d'un traitement particulier au sens de la proposition de Directive.

Pour ce faire, différents moyens se présentent à eux. Ils pourraient les transmettre par courrier ou utiliser des moyens traditionnels : télex, fax ou autres... Pour des raisons d'efficacité (normalisation des formats de transmission des messages), de confidentialité et de rapidité, ils s'adressent à S.W.I.F.T. qui met à leur disposition un réseau moderne de télécommunication.

Seuls les utilisateurs prennent la décision de communiquer ou pas les données à caractère personnel. De la même façon, le choix de l'organisme récepteur et celui des personnes concernées par les données est toujours effectué par l'utilisateur- émetteur. S.W.I.F.T. intervient uniquement pour concrétiser la volonté d'échange d'informations en fournissant un moyen particulièrement efficace.

Il semblerait dès lors raisonnable de voir en S.W.I.F.T. un agent traitant au service des différents responsables de fichier-utilisateurs. La finalité du traitement consisterait en la transmission des données à caractère personnel y compris les différentes opérations qui la rendent possible (enregistrement, conservation etc...).

La possibilité d'application du concept d'agent traitant à S.W.I.F.T. n'est cependant pas certaine. Les données à caractère personnel sont contenues dans des messages qui restent identiques d'un bout à l'autre de l'opération de transfert. On l'a dit, les données ne sont jamais extraites de ceux-ci en vu d'un regroupement ou d'une autre utilisation spécifique.

On est alors en droit de se demander en quoi consiste la tâche de S.W.I.F.T. vis-à-vis des données elles-mêmes. Ces dernières ne sont pas communiquées en tant que telles mais comme un élément parmi d'autres du message. Lorsque la proposition de Directive parle de communication, elle vise à garantir la protection de la personne concernée en grevant l'émetteur et le récepteur de certaines obligations. Lorsque la communication est interdite, c'est parce que par exemple la finalité du premier n'est pas compatible avec celle du second. Ce n'est pas l'opération de communication en elle-même qui est réglementée par la proposition. Ce sont les conséquences de celle-ci qui ont retenu l'attention des auteurs du texte, ce qui justifiait qu'elle soit reprise dans les opérations inhérentes aux traitements. Or, S.W.I.F.T. n'est ni un récepteur, ni un émetteur de données à caractère personnel, il en est seulement le transporteur occasionnel. La même réflexion peut se transposer qu'en cas du transfert de données à caractère personnel vers des pays tiers (article 24).

A cela, on pourrait répondre que le procédé utilisé, à savoir un réseau de communication géré et organisé de manière spécifique, implique que différentes opérations (conservation, enregistrement etc.) soient effectuées en annexe de l'opération principale de communication. Mais cette spécificité n'est-elle pas prise en compte dans la directive spécifique au secteur des télécommunications ?

Un argument de texte pourrait également être de nature à relativiser notre premier constat.

Au cas où le responsable du fichier transmettrait les données via un réseau, l'article 18.2 l'oblige à prendre des mesures propres à en assurer sécurité. Cette obligation pèse bien sur le responsable du fichier et non sur le gestionnaire du réseau de télécommunication utilisée. Elle grèvera de la même manière l'agent traitant agissant pour le compte du responsable du fichier. Ne peut-on y voir un signe de ce que le rédacteur du texte ne pensait pas que cet agent puisse être également le gérant du réseau utilisé ? Et dans ce cas, la raison n'est-elle pas à trouver dans le fait que, pour ce rédacteur, la solution est alors à trouver non pas dans la Directive générale mais bien dans la Directive spécifique aux réseaux de télécommunication (voir infra) ?

Évidemment, il est toujours hasardeux de supputer sur l'intention du rédacteur. Cela est d'autant plus vrai que le caractère flou des règles de la proposition laisse place à de nombreuses interprétations.

Section III : Conclusions concernant l'applicabilité aux données contenues dans les messages

A. Diverses interprétations possibles

Voir en S.W.I.F.T. un agent traitant plutôt qu'un maître de fichier reste le fruit d'une réflexion personnelle des auteurs de cette étude. Il paraît évident que différents pays intervenant dans le processus d'élaboration de la directive européenne considèrent qu'elle s'appliquera au réseau S.W.I.F.T. La lecture des concepts que nous proposons ici permet, nous le pensons, de soutenir une thèse différente. A tout le moins, elle met en lumière l'inadéquation certaine des concepts utilisés dans la Proposition au cas d'application à un réseau de transmission de messages comprenant des données à caractère personnel[71].

Ainsi, comme il a été dit plus haut, S.W.I.F.T. ne peut pas être appréhendé par la notion de "responsable de fichier" si ce n'est dans le cas où les données à caractère personnel sont traitées pour des finalités spécifiques.

Même si l'application du concept d'agent traitant à S.W.I.F.T. ne semble pas tout à fait adéquate (voir supra), elle paraît cependant la plus raisonnable et la plus proche de la réalité.

Remarquons enfin qu'il semble bien que la protection de la personne concernée par les messages doive plutôt être garantie par le biais des législations sur le secret des correspondances.

B. Le Secret de la correspondance

S.W.I.F.T. met son réseau à la disposition des utilisateurs et offre un service de transmission de messages. Il est dès lors tenu respecter le secret de la correspondance.

---

71 Cette constatation a été également faite en France quoique d'une manière un plus ambigüe. Voir LAMY-DROIT DE L'INFORMATIQUE, *Secret des télécommunications et protection des données nominatives des correspondants,* Lamy, Paris, 1992, n°1421, p.902. En parlant de la loi du 6 janvier 1978 (loi générale en matière de traitements de données nominatives) et de la loi du 8 janvier 1988 rela tive à la fraude informatique, les auteurs reconnaissent que "ces textes ne concernent pas directement la circulation des données à partir de réseaux de télécommunications".

Cependant, la question du secret de la correspondance sortant du champ limité de cette étude, nous nous limiterons à en rappeler l'essentiel sans prétendre la traiter de manière exhaustive.

Le principe du secret de la correspondance est affirmé dans de nombreuses conventions internationales[72] et se retrouve dans la plupart des législations nationales. Il s'applique aux correspondances privées émises par la voie de télécommunication (secret des télécommunications), sans égard à la manière dont celles-ci ont lieu. Les législations les plus récentes protègent par le biais du secret des télécommunications la transmission de tout signal, écrit, image, son, renseignement de toute nature[73]. Il importe peu que la transmission ait lieu de façon électronique[74]. Tous les réseaux de télécommunications sont compris y compris les réseaux informatiques. La protection couvre ainsi de manière générale toute correspondance émise par voie de télécommunication.

Le secret de la correspondance paraît donc bien devoir s'appliquer à l'échange de messages financiers informatisés via le réseau de télécommunication géré par S.W.I.F.T.. En vertu de ce principe, le respect de la confidentialité du contenu des messages doit être assuré par toute personne. Il ne peut y être porté atteinte que dans des cas exceptionnels. En outre, l'ingérence dans le contenu de la correspondance nécessite normalement l'adoption de garanties appropriées. Ainsi, par exemple, certains pays requièrent l'intervention d'un juge.

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

Même si S.W.I.F.T. ne peut être considéré comme responsable de fichier opérant un traitement sur les données à caractère personnel contenues dans les messages, il n'échappe pas à toute obligation. En effet, nous verrons que S.W.I.F.T. peut être qualifié de responsable de fichiers constitués des données relatives aux utilisateurs et générées par l'utilisation de son réseau Il convient d'effectuer une distinction entre d'une part, l'application de la proposition de directive spécifique aux télécommunications (section I) et d'autre part, celle de la directive générale (Section II).

---

72 Article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales; Déclaration universelle des droits de l'homme des Nations Unies adoptée en 1948.

73 Loi française du 10 juillet 1991.

74 Voyez par analogie ce qui est dit au sujet du courrier électronique in "les nouvelles technologies un défi pour la protection de la vie privée, conseil de l'Europe, Strasbourg, 1989, p.31.

Section I : La proposition de Directive "télécoms"[75]

A. Introduction

S.W.I.F.T. pourrait être considéré comme responsable de fichier de données provenant de l'utilisation du service de télécommunication. On ne s'intéresse plus ici aux données à caractère personnel contenues dans les messages circulant sur le réseau géré par S.W.I.F.T. mais bien aux données à caractère personnel nécessaires à ou crées par l'utilisation du réseau de télécommunication. Les données collectées dans ce cas par S.W.I.F.T. seront pour des raisons évidentes mises en rapport avec l'utilisateur, que ce dernier soit ou non une personne physique. L'exemple le plus significatif à cet égard est constitué par les données recueillies et traitées en vue de facturer le service rendu. Ainsi S.W.I.F.T. disposera des coordonnées complètes de l'utilisateur, du type de message émis, et de la date voire même de l'heure exacte de l'émission du message.

Dès lors, et dans la mesure où il est d'ores et déjà acquis que le champ d'application de la directive "télécoms" sera étendu aux fournisseurs privés de services de télécommunications, S.W.I.F.T. sera tenu de respecter les prescrits de ce texte. A ce stade, il convient donc d'en exposer les points principaux et d'examiner son impact sur S.W.I.F.T. tout en gardant à l'esprit que l'extension du champ d'application entraînera vraisemblablement la réécriture voire même la modification de la portée de certaines des dispositions commentées.

B. Contexte

La proposition de directive relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui jusqu'ici a constitué la référence de notre analyse, a été conçue comme une directive-cadre. Le texte est complété par diverses mesures visant à apporter une protection aussi complète que possible dans des domaines spécifiques. Ainsi, suite aux risques d'atteintes à la vie privée auxquels peuvent donner lieu la numérisation des réseaux et la mise en circulation du R.N.I.S., une directive sectorielle a été proposée dans le domaine particulier des télécommunications. Ce texte vise à appliquer les principes de la directive générale dans un domaine spécifique et à répondre aux besoins propres aux nouveaux réseaux de télécommunications. Il s'agit de la proposition de directive du Conseil concernant la protection des données à caractère

---

75 Proposition de directive du Conseil concernant la protection des données à caractère personnel et de la vie privée dans le contexte des réseaux de télécommunications numériques publics, en particulier du réseau numérique à intégration de services (RNIS) et des réseaux numériques mobiles publics, document COM (90) 314 final-£SYN 288; ci-après dénommée directive "télécoms".

personnel et de la vie privée dans le contexte des réseaux de télécommunications numériques publics, en particulier du réseau numérique à intégration de services (RNIS) et des réseaux numériques mobiles publics[76]. Dans l'état actuel, ce texte ne concerne que les réseaux de télécommunication publics.

La proposition de directive "télécoms" vise à assurer la protection de la vie privée principalement de deux manières. D'une part, elle limite les possibilités de stockage et de traitement des données dans le cadre de l'exploitation des télécommunications publiques à ce qui est nécessaire pour assurer un service de qualité et une gestion efficace. D'autre part, elle garantit à l'abonné un droit de l'abonné à "l'autodétermination informationnelle" tant à l'égard l'organisation de télécommunications que vis-à-vis des tiers en ce compris les autres abonnés.

C. Champ d'application

La directive "télécoms" réglemente de manière spécifique la collecte, le stockage et le traitement des données à caractère personnel par des organisations des télécommunications dans le cadre de la fourniture de services publics de télécommunications au sein des réseaux publics de télécommunications numériques dans la Communauté, et en particulier via le RNIS et les réseaux mobiles numériques publics[77].

Toutefois, il faut rappeler qu'il est largement admis que le champ d'application sera élargi. Ainsi, le Parlement a voté un amendement visant à modifier le titre de la directive pour englober les réseaux numériques mobiles publics ou privés et les services à valeur ajoutée publics et privés[78].

Par ailleurs, bien que les dispositions s'orientent essentiellement vers la téléphonie vocale[79], la directive prévoit qu'elles s'appliquent également à d'autres services de télécommunications "dans la mesure où ces services présentent des risques similaires pour la vie privée de l'utilisateur "[80].

---

76 (section I).

77 Article 2

78 Amendement n° 96 du Parlement européen, Procès-verbal de la séance du mercredi 11 mars 1992, 1992-1993, doc. PE 160.503.

79 COM (90) 314 final-SYN 287 et 288, 13 septembre 1990, p.90.

80 Article 19

D. Définitions

La proposition de directive définit les concepts de base nécessaire à l'application des principes. Ainsi, il est précisé ce qu'il faut entendre par "données à caractère personnel", les "organisations des télécommunications", le "réseau public de télécommunications" ou encore le "service public de télécommunications"[81].

La définition de "données à caractère personnel" n'est pas identique à celle reprise dans la directive générale. Il s'agit pour l'application de la directive "télécoms" de "toute information concernant une personne identifiée ou identifiable". On le voit, la notion est bien plus large que dans la directive générale où il était question "toute information concernant une personne physique identifiée ou identifiable". Les données, objet de la réglementation s'étendent donc à toute personne et ne sont plus limitées aux seules personnes physiques. Dans la mesure où la directive viendrait à s'appliquer aux prestataires de service privés, ce seraient donc les données concernant tout utilisateur du réseau de télécommunications qui seraient soumises aux dispositions de la directive.

E. Principe de finalité

L'article 4 de la proposition de directive précise comment le principe de finalité doit être compris dans le domaine des télécommunications. Il prescrit que la collecte, le stockage et le traitement de données à caractère personnel ne peuvent avoir lieu que s'ils peuvent se justifier "à des fins de télécommunications" et "à d'autres fins opérationnelles légitimes". Le même article détermine également ce qu'il faut entendre par "fins de télécommunication". Il s'agit en particulier de l'établissement de connexions pour la transmission de la voix, de données ou d'images, l'établissement de factures et la réalisation d'annuaires. Les "fins opérationnelles légitimes" concernent, quant à elles, la correction d'erreurs, la prévention de l'utilisation inappropriée de l'équipement d'une organisation de télécommunications etc...

Par ailleurs, l'article 5 précise que les données ne peuvent être enregistrées que si cela s'avère nécessaire pour "conclure, exécuter, modifier ou mettre fin au contrat avec l'organisation des télécommunications". Il énonce encore que les données ne peuvent être conservées pour une durée excédant celle du contrat sauf pour des répondre à des plaintes, récupérer des redevances ou pour d'autres finalités particulières spécifiées.

---

81 Article 3

Il est enfin à remarquer que l'article 5 exclut toute possibilité de stockage du contenu des d'informations après la fin de la transmission. Il est toutefois permis aux Etats-membres de déroger à cette interdiction, mais ils ne peuvent le faire que "conformément au droit communautaire".

Le principe de finalité reçoit une application particulière en matière de facturation détaillée.

F. Facturation détaillée

La collecte de certaines données relatives aux abonnés par les opérateurs de réseau et les fournisseurs de services est nécessaire pour permettre la facturation des services offerts. Les informations concernent essentiellement le numéro de téléphone de l'abonné appelé et appelant, l'heure de début et de fin de chaque appel ainsi que le service de télécommunications utilisé par l'abonné. La facturation détaillée est un service rendu à l'abonné, qui en tant que consommateur doit pouvoir vérifier la facture qui lui est adressée. Toutefois, pareille facilité présente certains dangers en regard de la protection de la vie privée de l'abonné. Les articles 9, 10 et 11 de la proposition de directive visent à résoudre le conflit qui pourrait exister entre ces deux intérêts difficilement conciliables.

Les données dites "de trafic", devront en principe être effacées après l'interruption de l'appel, sauf si elles sont rendues anonymes ou restent nécessaires à des fins de facturation ou à d'"autres fins légitimes".

Toutefois les informations de facturation pourront être enregistrées et traitées pour autant que le stockage n'excède pas le délai légal de contestation de la facture.

En vue de protéger la vie privée des abonnés appelés, il a en outre été prévu de supprimer les quatre derniers chiffres des numéros des abonnés appelés.

Appliquée à S.W.I.F.T., cette disposition impliquerait que le stockage des données de facturation soit limité et que les factures envoyées ne comprennent pas les derniers chiffres des numéros appelés.

G. Droit d'information de l'abonné

L'abonné dispose d'un droit d'accès et de rectification aux données enregistrées le concernant. Il a ainsi le droit de savoir si des données le concernant sont stockées et traitées, il peut même en obtenir la communication sous une forme "intelligible"; il peut

enfin en obtenir la rectification ou l'effacement si elles sont traitées en violation des dispositions imposées par le droit des états membres ou la législation communautaire[82].

Pareil principe, s'il devait être appliqué à S.W.I.F.T. obligerait ce dernier à laisser les utilisateurs accéder aux données enregistrées les concernant. S.W.I.F.T. serait également tenu de rectifier, à leur demande, le cas échéant, les données erronées ou traitées en violation de la réglementation établie.

H. Sécurité du réseau

L'organisation de télécommunication est tenue d'assurer la protection adéquate des données à caractère personnel contre l'accès et l'utilisation non autorisés. Le niveau requis est celui correspondant à l'état de la technique. Dans certains cas de risque particulier de violation de la sécurité d'un réseau, comme par exemple dans le domaine de la radiotéléphonie mobile, l'organisation de télécommunications doit informer l'abonné des dangers et lui offrir un service de chiffrement de bout en bout[83].

Il ne semble pas a priori que cette disposition soit susceptible de créer des difficultés particulières dans le cas où la directive s'appliquerait au réseau S.W.I.F.T. En effet, des mesures spécifiques de sécurité sont appliquées lors de la transmission des messages.

I. Identification de l'appelant

La proposition de directive appréhende le problème particulier posé par les nouvelles fonctions offertes par les services téléphoniques. L'article 12 énonce que l'abonné appelant doit avoir la possibilité de supprimer l'affichage de son numéro de téléphone sur l'appareil de l'abonné appelé. Il en va de même en ce qui concerne la transmission du numéro de téléphone. De manière similaire, l'abonné appelé doit pouvoir supprimer l'affichage sur son terminal des appels entrant.

Ce principe ne devrait pas poser de problème dans le cas de S.W.I.F.T. puisque l'utilisation du réseau repose sur la reconnaissance réciproque des parties. On imagine difficilement les cas où soit l'appelant soit l'appelé veuille supprimer son identification.

Section II : Application de la directive générale

---

82 Article 6
83 Article 8

Remarquons tout d'abord que la directive générale reste d'application dans les cas qui ne sont pas spécifiquement traités dans la directive télécoms[84].

Le cas visé ici est celui où l'utilisateur du réseau S.W.I.F.T. est une personne physique. Des données à caractère personnel la concernant risquent d'apparaître dans des fichiers. Les informations se rapporteront à son identification et les types de services que S.W.I.F.T. lui fournit. Ces renseignements peuvent être très précis dans la mesure où ils contiennent la fréquence, le type de messages émis ainsi que l'heure de leur transmission. Les informations nominatives sont vraisemblablement enregistrées et conservées pour des finalités de transmission des messages, de preuve et de facturation des services. Les fichiers sont dès lors susceptibles d'être interprétées comme autant d'informations faisant l'objet d'un traitement au sens de la proposition de Directive .

Il semble évident que dans ce cas S.W.I.F.T. apparaît comme le responsable du fichier. Prenons l'exemple du fichier servant à la facturation. Il est certain que S.W.I.F.T. effectue alors un regroupement de données particulières (le nombre de messages envoyés) qu'elle associe à une personne physique afin de calculer la somme due par cette dernière. Ce faisant, elle donne à ce regroupement une finalité particulière, gère et organise un fichier, décide des données qui y figurent et décide même des tiers qui pourraient y avoir accès. Elle agit donc bien en tant que responsable de fichier.

---

84 Proposition de directive du Conseil concernant la protection des donné"es à caractère personnel et de la vie privée dans le contexte des réseaux de télécommunications numériques publics, en particulier du réseau numérique à intégration de services (RNIS) et des réseaux numériques mobiles publics, considérant 21.

PARTIE III : EFFETS INDIRECTS DE LA PROPOSITION DE DIRECTIVE

Après s'être posé la question de l'applicabilité de la proposition de Directive au réseau S.W.I.F.T. lui-même, il paraît opportun de s'interroger maintenant sur les conséquences indirectes pour S.W.I.F.T. d'une telle application aux membres utilisateurs du réseau. Une fois le problème cerné (Section I), nous nous efforcerons de proposer certaines solutions (Section II).

CHAPITRE I : RISQUES DE DIMINUTION DE L'ACTIVITE DE S.W.I.F.T.

L'examen de la problématique des flux transfrontières de données à destination de pays tiers à la communauté européenne doit être envisagée dans le cadre de cette section.

Si S.W.I.F.T. ne peut être qualifié de responsable de fichier de données à caractère personnel, tel n'est pas le cas des utilisateurs du réseau. En tant qu'organismes financiers, ils possèdent généralement différents fichiers contenant des données à caractère personnel dont certaines vont être extraites et transmises afin d'effectuer certaines opérations. C'est à eux que revient la compétence de décider quelle sera la finalité de ces fichiers, quelles catégories de données à caractère personnel y seront enregistrées, quelles opérations leurs seront appliquées et quels sont les tiers qui peuvent y avoir accès.

Une fois que les principes prévus dans la future directive seront intégrés dans les diverses législations nationales, il ne fait aucun doute que la grande majorité des utilisateurs tomberont sous leur champ d'application.

Pour effectuer des opérations financières pour le compte de leurs clients, les utilisateurs du réseau doivent parfois transmettre des informations vers d'autres pays. Dans la mesure où ces informations comprennent des données à caractère personnel, les utilisateurs devront prendre en compte les principes prévus dans la proposition de directive en matière de flux transfrontières à destination de pays tiers.

La situation dans laquelle la directive s'appliquerait est la suivante : un utilisateur du réseau membre de la communauté européenne - responsable d'un fichier - transfère des

données à caractère personnel vers un pays tiers. Ainsi par exemple un banquier belge transmet par l'intermédiaire du réseau S.W.I.F.T. des données à caractère personnel à un banquier coréen à la demande d'une personne physique souhaitant effectuer un transfert de fond.

Si l'Etat tiers (la Corée dans l'exemple) n'assure pas aux données "un niveau de protection adéquat", l'article 24 de la proposition de directive précise que le transfert doit être interdit par le droit national de l'Etat-membre émetteur. Si l'on reprend l'exemple, c'est dans la réglementation belge que se trouvera pareille interdiction.

L'interdiction s'appliquera donc lorsque l'Etat vers lequel les données sont transférées ne garantit pas de protection estimée adéquate aux données. L'appréciation du caractère adéquat ou non de la protection accordée par le pays tiers importateur sera effectuée par ce pays européen (la Belgique dans l'exemple).

Comme nous l'avons mentionné plus haut[85], ce sera souvent au sein de chaque Etat membre, en fait à l'autorité de protection de données[86] que sera confié le pouvoir de trancher sur le niveau de protection. Elle sera amenée à connaître des communications de données et notamment de celles destinées à l'étranger (il s'agirait dans l'exemple de la Commission vie privée belge) .

Deux cas de figure peuvent alors se présenter. Soit la protection est jugée adéquate, et normalement le transfert de données sera avalisé. Soit l'Etat membre estime la protection offerte par le pays tiers non adéquate, il bloquera alors le transfert et informera la Commission des Communautés Européennes[87]. C'est bien ici que se situe le noeud problème puisque le responsable du fichier -utilisateur du réseau- risque de se voir interdire le transfert des données. Dans la mesure où pour effectuer cette transmission, il fait appel au réseau S.W.I.F.T., ce dernier en subira indirectement les conséquences puisque le nombre de messages envoyés diminuera en proportion. Une autre conséquence de cette interdiction sera l'infirmation de sa capacité de transférer les messages financiers dans n'importe quel pays du monde, ce qui représente, aujourd'hui, un de ses attraits principaux.

Rappelons que c'est sur la base des informations fournies par les Etats membres, ou éventuellement à partir d'autres renseignements, que la Commission pourra constater que

---

85 voir la partie exposant la façon dont la proposition de directive aborde la question des flux transfrontières de données.

86 Article 26

87 Cette information doit être comprise au regard du rôle de la Commission en matière d'uniformisation des pratiques des Etats-membres.

le pays en question ne dispose pas d'un niveau de protection adéquat. Elle pourra alors entamer des négociations en vue de remédier à la situation.

La Commission pourra également décider qu'un pays tiers offre bien une protection adéquate[88]. Pour ce faire, elle aura pris l'avis du comité consultatif[89] et fondé son appréciation sur l'état de la législation interne et l'existence d'engagements internationaux souscrits par l'Etat importateur.

A l'interdiction de l'article 24, l'article 25 de la proposition de directive apporte une exception majeure.

L'Etat membre hôte du fichier peut autoriser le transfert "sur présentation par le responsable du fichier de justifications suffisantes pour garantir le respect d'un niveau de protection adéquat". Il s'agit de l'obligation à charge de l'exportateur européen, d'assurer par divers moyens la protection de la vie privée lorsque les données sont traitées à l'étranger. L'objectif poursuivi est de concilier le besoin d'échange d'information automatisée et les principes de protection des données.

La garantie la plus efficace semble être l'insertion de clauses contractuelles ad hoc dans une convention passée entre l'importateur et l'exportateur des données. Le contrat vise alors à obliger le destinataire à respecter les principes de protection des données appropriés, garantissant à la personne concernée une protection face aux traitement et à l'utilisation des données qui la concernent.

Rappelons enfin que, l'article 25 prévoit une procédure d'information de la Commission et des Etats membres et un délai de notification d'opposition de 10 jours. En cas de notification d'opposition, la Commission pourrait prendre les mesures appropriées et notamment aux termes de l'exposé des motifs, décider d'interdire le transfert des informations[90]. L'adoption de clauses contractuelles par les utilisateurs n'implique donc pas que l'utilisateur soit en tout état de cause autorisé à transférer les données.

---

88 Article 24 §4

89 Article 30

90 La Commission est tenue de prendre l'avis du Comité consultatif selon la procédure prévue à l'article 30 §2.

CHAPITRE II : PROPOSITION DE SOLUTIONS

En vue d'éviter les inconvénients auxquels l'application de l'article 24 pourrait donner lieu, il serait intéressant pour S.W.I.F.T. d'élaborer des clauses contractuelles auxquelles devraient adhérer les utilisateurs de son réseau. Parallèlement aux clauses ayant une importance commerciale directe, les utilisateurs s'engageraient à respecter les principes de base de la directive. Ces clauses pourraient être intégrées au contrat qui lie les utilisateurs au réseau S.W.I.F.T.

Cette solution ne constitue pas un remède miracle. Donner des droits à la personne concernée ne les rend pas opposables ipso facto aux parties au contrat. Le problème se posera lorsque l'importateur violera ses engagements sans que l'exportateur n'agisse contractuellement à son égard. L'effet relatif des contrats empêchera la personne concernée d'agir contre l'importateur récalcitrant. Dès lors, l'exportateur restera exposé au risque de se voir interdire la transmission des données. C'est pourquoi, il semble nécessaire de prévoir, à côté de la solution contractuelle, un système permettant de garantir l'application effective des clauses.

Section I : Les clauses contractuelles

A. Le type de clauses

Plus précisément, les clauses reprendraient une série d'obligations en matière de protection des données. Ainsi par exemple on devrait prévoir l'obligation de traiter les données de façon loyale et licite et de les stocker à des fins spécifiques et légitimes. Le destinataire des données ne devrait les utiliser que pour les fins nécessaires à la réalisation du service demandé par l'émetteur.

Des clauses au contenu plus spécifique devraient également être ajoutées. Il faudrait reconnaître à l'individu fiché le droit d'accéder aux données le concernant et, le cas échéant, de les faire rectifier.

En outre, pour que leur décision soit respectée par les tribunaux, les parties devraient choisir un système juridique spécifique et non pas mentionner une série de principes généraux adoptés par elles ou une série de règles qui n'appartiennent pas à un système

juridique[91]il faudrait prévoir des clauses d'interprétation et d'application du contrat. Ainsi on pourrait préciser la procédure à suivre en cas de litige entre les parties quant à l'interprétation correcte des dispositions. Une clause de choix de juridiction est utile. Il nous semble que la juridiction du pays de l'exportateur devrait être choisie.

Enfin, la mise en place d'une procédure d'arbitrage semble appropriée vu son accès facile et rapide et son caractère peu onéreux. Il ne faut cependant pas oublier qu'une clause d'arbitrage n'est obligatoire que pour les parties au contrat et non pour les tiers[92].

Avant de donner un contenu plus précis aux clauses, quelques observations essentielles doivent encore être formulées. Les clauses proposées ne permettent pas d'échapper à toute difficulté. La personne concernée par les données reste tiers au contrat et pourrait se voir dans l'impossibilité d'exercer ses droits à l'égard de l'importateur des données.

Divers mécanismes juridiques ont été proposés par la doctrine pour remédier à ce problème[93]. Malheureusement, ces solutions basées généralement sur un droit national particulier sont difficilement transposables à l'ensemble des ordres juridiques concernés par les flux. Un mécanisme juridique parfaitement valable dans un droit national spécifique ne l'est pas forcément dans un autre.

La solution la plus intéressante réside dans le mécanisme de la représentation. Un contrat serait conclu d'une part entre l'exportateur -au nom de la personne concernée- et d'autre part l'importateur. Les clauses "privacy" sont alors incluses dans un contrat annexe au contrat commercial de base.

Une clause de ce type pourrait être prévue : "considérant qu'il est entendu que l'exportateur est l'agent et le représentant autorisé des personnes concernées par les données à transférer en vertu de ce contrat ..."[94].

---

91 Eléments complémentaires sur l'avis élaboré par le Professeur Allan Philip, avocat, Pontoppidan, Philip et associés (Copenhague).

92 voy. comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caratère personnel du 28 janvier 1981, aspects contractuels des flux transfrontières de données, avec modèsles de contrats, éléments complémentaires sur l'avis élaboré par le Professeur Allan Philip, avocat, Pontoppidan, Philip et associés (Copenhague).

93 Pour une analyse globale, voir A. Bourlond, op. cit., spéc. P. 11 et suivantes et références citées.

94 Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, *propositions de clauses pour inclusion dans un contrat-type visant à assurer une protection équivalente pour des données à caractère personnel dans le cadre de flux transfrontière de données*, Strasbourg, le 18 mai 1990, T-PD (90) 24

Un lien direct s'établit alors entre la personne concernée et le destinataire ce qui permettra à la première d'agir en justice contre le second. Il n'en reste pas moins que la technique de la représentation n'est pas aussi aisée à mettre en oeuvre dans les législations de chacun des pays[95]. Ainsi par exemple, en droit anglais, il semble difficile de considérer le fournisseur de données comme agent représentant de la personne concernée. Pour que celui-ci puisse se faire, cette dernière (commettant) devrait avoir accepté préalablement que l'exportateur (agent) ait sur lui un pouvoir contraignant. L'existence d'un tel consentement sera difficile à établir sauf à imaginer que la personne physique, cliente de la banque exportatrice, remplisse une déclaration précisant que la banque est son agent pour les éventuels contrats de transmission de ces données à des tiers, ce qui paraît difficilement envisageable. Une telle solution nous paraît difficilement transposable au cas qui nous préoccupe.

B. Les clauses proposées

On peut proposer des clauses du type suivant[96] :

"Aux fins du présent contrat :

l'expression "données à caractère personnel" signifie toute information transmise par l'exportateur à l'importateur et qui concerne une personne physique identifiée ou identifiable (personne concernée).

L'exportateur déclare et garantit à l'importateur que les données sont :

- obtenues et traitées loyalement et licitement;

- enregistrées pour des finalités déterminées, explicites et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;

- adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées

- exactes et si nécessaire, mises à jour;

---

95 voy. A. Bourlond, op. cit., p. 12.

96 Les clauses sont largement inspirées d'un document du comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, *propositions de clauses pour inclusion dans un contrat-type visant à assurer une protection équivalente pour des données à caractère personnel dans le cadre de flux transfrontière de données*, op. cit.

- conservées sous une forme permettant l'identification des personnes concernées pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été enregistrées.

Sans que cette énumération ne soit limitative, l'importateur s'engage en particulier à respecter les obligations suivantes[97].

L'importateur ne fera pas usage des données pour des finalités ou activités autres que celles pour lesquelles elles ont été initialement et légalement fournies par l'exportateur.

L'importateur s'engage à permettre aux personnes concernées d'avoir accès aux données dont il a la responsabilité et s'engage à rectifier ou à effacer à leur demande dans un délai raisonnable les données qui seraient erronées ou incomplètes.

L'importateur s'engage à ce que les données soient traitées et conservées selon des mesures de sécurité détaillées.

Tout litige découlant de l'exécution des présentes clauses doit être soumis à l'arbitrage et à la décision d'un expert. Cet expert doit être sélectionné sur une liste d'experts établie par ....

Les parties conviennent, dans l'éventualité d'un différend lié à l'interprétation du présent contrat de le soumettre à la juridiction du pays de l'exportateur et d'accepter sa décision et toute autre stipulation annexe comme règlement complet et contraignant du différend. Les parties s'engagent à donner effet à toutes les décisions et à coopérer pleinement avec elle dans toutes les recherches qu'elle pourrait entreprendre en relation avec sa juridiction aux termes de la présente clause."

---

97 Il ne nous paraît pas opportun de prévoir une clause interdisant le traitement des données qui révèleraient l'origine raciale et ethnique, l'opinion politique, les convictions religieuses ou philosophiques, les appartenances syndicales ainsi que l'état de santé ou la vie sexuelle. En effet, si l'exportateur se limite à traiter les données en vue de répondre à la demande de l'exportateur, il ne sera pas amener à enregistrer des données sensibles. Les messages financiers ne devraient pas en contenir. Quid transfert de fichiers de sociétés ?

Section II : Un organe de contrôle ad hoc

Comme on l'a vu, les clauses contractuelles n'offrent pas toutes les garanties nécessaires pour assurer une protection adéquate. Les clauses telles qu'elles ont été présentées ne lient pas la personne concernée. A défaut d'un mécanisme juridique permettant de remédier à cette situation, deux solutions peuvent être envisagées afin de donner aux clauses un maximum d'effectivité.

La première consiste à prévoir dans le contrat liant S.W.I.F.T. et les utilisateurs une sanction applicable en cas de non-respect des clauses contractuelles "privacy". Ainsi, par exemple en cas de violation de ses obligations contractuelles, un utilisateur pourrait se voir exclu de l'utilisation du réseau S.W.I.F.T. Deux arguments plaident en faveur de l'adoption d'une clause de ce type. D'une part, elle illustre la volonté de S.W.I.F.T. de donner un caractère effectif à la protection établie. D'autre part, elle s'impose d'elle-même car il est préférable d'exclure un utilisateur du réseau que de s'exposer à se voir interdire le transfert vers un pays déterminé et par là de perdre une partie du marché.

Toutefois, cette solution n'est pas sans inconvénients. Rendre S.W.I.F.T. omnipotent en matière de sanctions aux violations des règles "privacy" pourrait heurter les membres utilisateurs. En effet, ceux-ci ne confient leurs messages au réseau qu'en vue de l'obtention d'un service spécifique, à savoir la transmission rapide et efficace de ceux-ci. Il semble dès lors préférable que S.W.I.F.T. conserve une certaine neutralité en cette matière. Dans le cas contraire, le rôle de police joué par le réseau paraîtrait incompatible avec sa mission première de dispensateur de service.

La seconde consiste en la création d'un organe indépendant à S.W.I.F.T. disposant d'un certain pouvoir de sanction à l'égard des utilisateurs. Cet organe serait composé de représentants des utilisateurs du réseau. Dans un souci de plus grande efficacité, ceux-ci devraient être choisis parmi les personnes compétentes en matière de "privacy" au sein des différentes institutions affiliées au réseau. S.W.I.F.T. y participerait en tant qu'observateur, certains pouvoirs pouvant lui être accordés. Les fonctions de cet organe seraient de deux types : contrôle et information sur les problèmes privacy.

En matière de contrôle, ses compétences s'étendraient à l'instruction des plaintes adressées par la personne concernée à l'encontre de l'importateur qui aurait violé les clauses. Pour ce faire, il devrait disposer des moyens d'investigation nécessaires à cette mission. S'il constate la violation, il devrait pouvoir sanctionner le membre fautif par exemple en le condamnent au versement d'indemnités à la personne concernée ou en

décrétant un boycott généralisé de tout transfert de données à l'institution en cause jusqu'à ce que celle-ci régularise la situation.

Il pourrait également se charger de rassembler et de dispenser l'information relative aux développements des réglementations "privacy" dans les différentes législations des Etats concernées par les flux. Ce dernière fonction n'est pas à négliger, il s'agirait de repérer les pays où les institutions "à risque" et cela avant toute intervention des institutions de contrôle nationales.

Dans le même ordre d'idées, elle pourrait contribuer à l'amélioration et à la mise en pratique des clauses contractuelles.

Cet instrument pourrait paraître a priori excessif. Cependant, il semble constituer la seule manière de se garantir contre toute interdiction d'exportation de données.

CONCLUSIONS

L'étude de l'applicabilité de la réglementation européenne "privacy" aux activités menées par S.W.I.F.T. n'a pas permis de dégager de certitudes. Cela est du principalement à l'utilisation de concepts de base dont les contours sont particulièrement flou. Si l'analyse effectuée a voulu démontrer que S.W.I.F.T. peut difficilement être qualifié de responsable de fichier, qu'il ne peut être totalement assimilé à un agent traitant, il n'en reste pas moins qu'une argumentation pourrait être développée visant à prouver l'inverse. Cette étude doit donc être prise avec certaines précautions. Et cela d'autant plus que le problème de l'application des réglementations privacy à un réseau de transmission de messages n'a jamais été envisagé en tant que tel.

On ne peut non plus perdre de vue que la proposition ne donne que les principes généraux d'une protection minimale à intégrer au sein des Etats membres. En mettant en oeuvre la directive dans leur droit national, ceux-ci restent libres d'interpréter les notions en cause, voire de compléter les garanties offertes à la personne concernée par les données à caractère personnel. Aussi, existe-t-il un risque de voir certains Etats décréter l'application de ceux-ci au réseau S.W.I.F.T. en le considérant, par exemple, comme un responsable de fichier à part entière ou en intégrant dans son champ d'application les données relatives ou personnes morales. Aussi, on ne peut que conseiller aux responsables du réseau d'être particulièrement attentifs à tout développement législatif "privacy" au sein des Etats où S.W.I.F.T. mène ses activités.

Il est à noter cependant que les Etats membres, une fois l'intégration des principes de la future directive dans les législations nationales effectuée, ne peuvent en aucun cas arguer d'une protection plus élevée pour restreindre les flux transfrontières de données au sein de la Communauté[98].

Quoiqu'il en soit, l'environnement juridique dans lequel se situe le réseau S.W.I.F.T. est en pleine mutation. Les réglementations "privacy", que ce soit au niveau européen ou au niveau des Etats-membres sont de plus en plus présentes, et doivent être prises en compte par S.W.I.F.T. lors de toute activité impliquant un traitement de données à caractère personnel.

---

98 Voir Exposé des motifs, COM (90) 314 final SYN 287 (13 septembre 1990), p.19 et 20.