La dimension internationale des services télématiques professionnels

Schaff, Sylvie

Publication date:
1986

Document Version
le PDF de l'éditeur

SS - II /

9

LA DIMENSION INTERNATIONALE DES SERVICES TELEMATIQUES PROFESSIONNELS

Sylvie SCHAFF,
Attachée de Recherches
au C.R.I.D.
Mars 1986.

Le texte qui suit présente des résultats des Actions Nationales de Recherche en soutien à FAST (Services du Premier Ministre - Programmation de la Politique Scientifique) - La responsabilité scientifique est assumée par son auteur.

LA DIMENSION INTERNATIONALE DES SERVICES

TELEMATIQUES PROFESSIONNELS

Section 1 : Le droit international applicable

Paragraphe 1 - La libre circulation des données
A - Enoncé du principe
B - Un droit fondamental de l'être humain
C - Une condition du développement du commerce international

Paragraphe 2 - La protection des données
A - Les données nominatives
B - La propriété intellectuelle

Paragraphe 3 - La normalisation
A - La normalisation technique
B - La normalisation administrative

Section 2 : Sa mise en oeuvre au niveau national

Paragraphe 1 - La protection de la souveraineté

Paragraphe 2 - Les réglementations nationales

Paragraphe 3 - La détermination de la loi applicable

L'intérêt de la télématique étant de faciliter les transferts de données informatiques, elle se situe par nature dans le contexte international. En effet, l'utilité de pouvoir communiquer les informations vite et loin ne se conçoit que pour des partenaires éloignés et en faisant abstraction des frontières nationales. Aussi le droit doit-il tenir compte de cette réalité, et appréhender les services télématiques professionnels comme étant avant tout des activités internationales (1).
Le principe général du droit qui s'adresse le plus directement à ces services est certainement celui de la libre circulation des données, tel qu'il est consacré par plusieurs textes internationaux dont la Déclaration des Droits de l' Homme et l'Accord Général sur les Tarifs et le Commerce (G.A.T.T.).

A l'énoncé de ces textes, on comprend que la libre circulation des données est à la fois l'un des droits fondamentaux de l'être humain (droit de s'exprimer, d'avoir accès aux réseaux de télécommunication) et une condition essentielle du développement du commerce international et du progrès en général, non seulement par la diffusion du savoir mais aussi par l'harmonisation des activités et par l'accélération et la meilleure efficacité de la prise de décision.

Il faut distinguer cependant la circulation des données de leur diffusion. Alors que la première vise seulement leur transfert, la seconde implique une multiplication du nombre de personnes en ayant connaissance : si une meilleure circulation des données permet leur diffusion sur une plus grande échelle, elle améliore également les échanges d'informations confidentielles (commerciales, financières, ...).
Or en matière de services télématiques professionnels, c'est le second aspect de la circulation des données qui importe. C'est pourquoi ce chapitre consacrera plusieurs sections à la protection des données transmises vers l'étranger.

Sur le plan économique, on remarque que l'industrie internationale des services télématiques est encore jeune. Son chiffre d'affaires était en 1983 d'environ 2 milliards de dollars, ce qui représente seulement 1/20 de celui des industries du même secteur (sociétés d'informatiques, conseils et services informatiques, télécommunications). De plus, elle croît actuellement à une vitesse moindre que ces autres industries (2).
Cela tient en particulier à ce que les frontières de l'industrie des services télématiques sont mal déterminées du fait qu'un grand nombre d'informations sont considérées comme faisant partie du domaine public et sont fournies

gratuitement, en particulier par les administrations. Ainsi on peut estimer à 30 milliards de dollars les dépenses publiques affectées à ce poste.
De même, de nombreuses entreprises considèrent leur système d'information comme une activité interne et n'envisagent pas de le proposer sur le marché, même s'il est utilisable et rentable.
Enfin, on constate qu'au niveau international, le commerce d'informations automatisées est proportionnellement beaucoup moins développé qu'au niveau national.

Cette industrie subit actuellement des transformations: les fournisseurs proposent de plus en plus de services à valeur ajoutée (stockage, courrier électronique, conseils, ...).
Il en résulte un changement dans leur type de clientèle. Alors qu'avant il s'agissait essentiellement de bibliothèques et centres de documentation et de recherche, les nouveaux clients sont plutôt des professionnels de certains secteurs spécifiques, agents de change, juristes, comptables, ... D'où la possibilité que le service concerné finisse par être intégré dans la profession à laquelle il s'adresse, comme c'est le cas pour les banques aujourd'hui, qui consacrent une grande part de leur activité à des opérations télématiques (de même pour les agents de change).
L'autre possibilité est que les services télématiques soient intégrés dans les industries voisines, telles les sociétés informatiques ou les télécommunications. C'est le cas par exemple du vidéotex.
On peut en tous cas affirmer que l'industrie des services télématiques va connaître une croissance considérable dans les prochaines années.

Du point de vue technologique, le développement de cette industrie s'opère dans trois directions.
- l'accroissement des possibilités (il est aujourd'hui plus facile d'accéder aux informations, de les traiter et les stocker, les ordinateurs sont de plus en plus puissants et les réseaux de télécommunications plus performants);
- le développement des ordinateurs personnels, qui élargissent considérablement le marché des services télématiques;
- l'expansion rapide des nouveaux moyens de transmission de données (3).

Cette expansion de l'industrie des services télématiques entraîne une modification de ses pratiques, notamment en raison de considérations juridiques. Alors qu'auparavant ces services étaient créés et utilisés par un nombre restreint de spécialistes, ils deviennent de plus en plus commerciaux et impersonnels et requièrent une "professionnalisation" des fournisseurs qui n'est malheureusement pas toujours atteinte.

Parmi les critiques qui leurs sont le plus souvent adressées, on note en particulier l'inadaptation des services de télécommunication, les pratiques abusives, le manque de documentation, la lenteur des mises à jour, le manque de fiabilité et les restrictions d'accès.

D'où l'importance de dégager les principes juridiques internationaux applicables en la matière.En effet l'absence de règles généralement admises non seulement nuit au développement de l'industrie des services télématiques et du secteur tertiaire en général, mais également à celui des secteurs primaires et secondaires par les freins qu'elle met à l'utilisation des nouvelles technologies.

La réalisation d'opérations télématiques internationales donne lieu à ce qu'on appelle les "flux transfrontières de données" (F.T.D.), c'est-à-dire "...des communications point-à-point entre des organes liés par des relations juridiques ou contractuelles et les données transférées ont souvent un caractère réservé" (4).
Cette définition appelle plusieurs remarques :
- les médias sont expressément exclus de notre analyse des F.T.D., dans la mesure ou leur but est la diffusion de messages destinés au public et non à un individu spécifique (qui a passé un contrat et est par là connu du fournisseur du service télématique);
- les F.T.D. ont toujours existé, sous forme de papier, communications téléphoniques, télex, ...) et la télématique ne représente qu'un nouveau moyen de les effectuer;
- le caractère international ou "transfrontière" de ces flux n'est qu'une dimension des flux de données (qui les distingue des flux nationaux).

On peut diviser les flux de données en trois catégories (5):
- les flux internes à une organisation (entreprise, ...)
- les flux entre organisations (fournisseur, client,...)
- les services télématiques.

Les deux premiers types de flux sont générés à l'occasion d'une autre opération du commerce international, entre des partenaires ayant d'autres relations commerciales. Ce sont essentiellement des opérations entre une société mère et ses filiales (gestion, coordination...) ou entre une entreprise et son client (réservation de places d'avion, transferts électroniques de fonds).
Les services télématiques par contre ont pour objet principal un flux de données (information, message ou traitement à distance), qui constitue une des bases de l'accord entre les parties. Ce sont eux qui constituent l'industrie des services télématiques dont nous avons parlé.

Dans les deux premiers cas, les F.T.D. sont un aspect nécessaire mais pratiquement invisible de l'opération : il est rare qu'ils donnent lieu à une comptabilité, encore plus à une facturation distincte. Pour les services télématiques par contre, le transfert de données est le but de l'opération et c'est pourquoi on les apparente parfois à des services de télécommunication (surtout en matière de messagerie électronique).

Enfin en ce qui concerne leur contenu, on distingue traditionnellement les flux de données nominatives des flux de données commerciales (6).

Les flux de données nominatives ont les premiers suscité des inquiétudes au niveau politique, ce qui explique que les discussions à leur sujet soient plus avancées et aient abouti à l'adoption de textes juridiques nationaux et internationaux restreignant la collecte et l'utilisation de telles données.

Ces flux ne représentent cependant qu'une part infime des F.T.D. en général, non en raison des réglementations restrictives qui les touchent, mais simplement de leur manque d'intérêt pratique : les F.T.D. sont le fait d'entreprises, qui communiquent des données commerciales (commandes, factures, fonds, ...). Pour ces entreprises, le développement du commerce international repose à la fois sur une meilleure circulation et une meilleure protection des données transmises.

Il apparaît ainsi que deux principes souvent présentés comme contradictoires, la libre circulation des données et leur protection, sont en fait complémentaires (cf. introduction).

Affirmer la libre circulation des données (commerciales ou autres) signifie que les échanges d'informations ne doivent pas être entravés par les Etats (par des restrictions en matière de télécommunication par exemple) mais qu'ils doivent au contraire être facilités, et en particulier être protégés contre les accès illicites par les tiers aussi bien que par les autorités publiques lorsqu'il s'agit de données confidentielles.

Si ce raisonnement est accepté au niveau international, comme le montre l'existence de principes généraux et de règles matérielles dans ce sens (section 1), son application au niveau national se heurte souvent à la susceptibilité des Etats en matière de souveraineté (section 2).

SECTION 1 - Le droit international applicable

Paragraphe 1 : La libre circulation des données

A. Enoncé du principe

Le principe de la libre circulation des données exprime un idéal en matière de flux transfrontières d'informations et présente deux aspects : l'absence de tout obstacle d'ordre juridique, technique, économique ou autre opposés aux F.T.D. et la prise de mesure favorisant ces flux (7).

Considéré dans son acception la plus large, ce principe est l'un des fondements du "nouvel ordre informationnel international" tel qu'il est discuté aujourd'hui au sein de l'U.N.E.S.C.O. et dont l'objectif est une meilleure répartition de l'information (et du pouvoir qu'elle apporte) entre les pays.
Cette approche entre dans le cadre plus large de la recherche d'un nouvel ordre économique international entreprise depuis plusieurs années. Elle devrait aboutir à introduire un certain nombre de règles de conduite adressées aux Etats et de mesures pratiques afin de réduire le déséquilibre actuel.

Le concept de la libre circulation des données est énoncé par la Déclaration Internationale des Droits de l'Homme (art. 18, 19 et 20) et signifie un engagement des Etats à améliorer l'accès aux informations de toute sorte à travers le monde, à garantir un droit de communication, la liberté d'expression et la liberté de la presse (8).
Ce concept peut cependant être interprété de plusieurs façons, notamment du fait qu'il a un impact certain en matière de souveraineté (cf. infra section 2). Son interprétation la plus libérale postule pour la réduction au minimum des contrôles gouvernementaux sur l'échange de données et d'informations. Il n'est cependant jamais question de priver de protection juridique les informations qui ont droit au secret ou de laisser impunie la divulgation d'informations fausses ou nuisibles.
La plupart des lois nationales contiennent des dispositions à cet effet (interdiction de la diffamation, de l'incitation au racisme, contrôle de la publicité, ...) et reconnaissent la nécessité de protéger certaines données (données nominatives, secret d'Etat, propriété intellectuelle, ...) et les textes internationaux, notamment la Déclaration des Droits de l'Homme, révèlent un large consensus des pays sur le bien fondé de cette protection.

S'il est admis que le principe de libre circulation des données doit nécessairement être circonscrit à certaines limites, les méthodes pour le mettre en oeuvre sont controversées.
Certains pensent qu'il vaut mieux partir d'une présomption favorable aux flux de données et prévoir des sanctions applicables à postériori en cas d'accès illicite à des données protégées.
Pour les autres au contraire, laisser aux utilisateurs la liberté de faire ce qu'ils veulent sans les avertir des conséquences possibles aboutirait à une limitation superficielle des flux d'information et il serait préférable d'élaborer une réglementation de la libre circulation des données indiquant clairement son cadre et ses limites.

Si cette controverse n'a pas encore reçu de solution, on trouve déjà parmi les principes traditionnels du Droit International des dispositions qui impliquent ou qui favorisent la libre circulation des données, reconnue comme un droit fondamental de l'être humain et une condition du développement du commerce international.

B. La libre circulation, droit fondamental de l'être humain

La liberté d'expression et de communication, reconnue par les articles 18, 19 et 20 de la Déclaration Internationale des Droits de l'Homme, est mise en oeuvre en matière télématique par le droit du public d'utiliser les systèmes et équipements de télécommunication qui figure à l'article 18 de la Convention Internationale des Télécommunications.

> "Les membres reconnaissent le droit au public de correspondre par le truchement du service international de correspondance publique. Les services, les charges et les garanties seront les mêmes pour tous les utilisateurs dans chaque catégorie de correspondance sans aucune priorité ou préférence" (9).

Cette convention reconnait donc à la fois le droit pour tous d'utiliser le réseau de télécommunication et l'obligation d'accorder le même traitement à tous les utilisateurs d'une même catégorie.
On peut en déduire le droit des fournisseurs de services télématiques professionnels de fournir ces services, dans leur pays et à l'étranger, et celui des utilisateurs de faire appel à de tels services, nationaux ou étrangers. On en déduit également l'égalité de traitement entre les

fournisseurs nationaux et étrangers, principe qui est repris dans plusieurs conventions sur le commerce international (cf. infra).

Ce principe interdit en particulier que des considérations autres que de nature technique soient prises en compte pour la concession de lignes de télécommunication. En matière de services télématiques, on peut penser à des restrictions fondées par exemple sur le type de données transmises ou sur la nationalité de leur fournisseur.
Mais le principe du libre accès au réseau ne permet pas de mettre en cause les restrictions indirectes aux télécommunications, comme leur structure tarifaire par exemple, même s'il interdit les formes les plus grossières de censure.

C. La libre circulation, condition de développement du commerce international

La libre circulation des biens et des services est depuis longtemps reconnue comme une condition indispensable du développement du commerce international, et constitue le fondement de l'Accord international le plus important aujourd'hui en matière économique : le G.A.T.T. (General Agreement or Tariffs and Trade), dont l'objectif à long terme est la suppression des droits de douane et des obstacles non tarifaires à la libre circulation des marchandises.

Que l'information soit considérée comme un bien (cf. introduction), comme un service ou comme ayant une nature spécifique, il ne fait aucun doute que l'amélioration de sa circulation bénéficie au commerce international. On peut en citer plusieurs exemples :
Grâce à cette amélioration, les commerçants et entrepreneurs sont au courant des marchés internationaux de façon plus complète et plus rapide. Ils peuvent contacter la personne responsable et conclure la transaction à distance, par téléphone, télex... Enfin la réalisation de l'opération est également facilitée, puisque les documents commerciaux (commande, facture, ...) et le paiement seront transmis rapidement et sûrement.
Les services télématiques participent entièrement à ce développement, ce qui permet d'affirmer l'application des principes du commerce international à leur endroit.

1) On peut citer en premier lieu les principes tendant à maintenir le jeu de la concurrence contre l'interventionisme des Etats ou l'abus de position dominante.

Le premier d'entre eux est le principe du traitement national des intérêts étrangers, qui interdit la discrimination contre des personnes, des biens ou des services en raison de leur origine étrangère (10).
Ce principe est reconnu par plusieurs conventions internationales, telles le G.A.T.T., la Convention Universelle sur les Droits d'Auteur (Berne) et la Convention pour la Protection de la Propriété Industrielle (Paris).
Il implique que les services télématiques étrangers devront bénéficier dans un pays de la même protection et du même traitement que les services nationaux.

On remarque cependant que le principe du traitement national n'est pas universellement admis en matière de flux transfrontières de données, qui peuvent être soumis à des restrictions. Par exemple, la loi brésilienne de 1984 sur l'informatique stipule que "les services informatiques de gestion ne peuvent être offerts (par des étrangers)que dans la mesure où les services visés ont un caractère réellement international" (11) et établit ainsi une discrimination à l'encontre des fournisseurs étrangers de services télématiques.
Les raisons de telles discriminations sont à la fois politiques (sauvegarde de la sécurité nationale et de l'identité nationale) et économiques : l'acceptation du principe du traitement national interdit d'accorder un traitement privilégié aux entreprises nationales et de promouvoir ainsi leur développement.

. Il faut noter ici que si ce type de réglementation est applicable aux fournisseurs de services télématiques établis dans le pays en question, il est par contre difficile à appliquer aux services fournis de l'étranger par le réseau de télécommunication, ce qui est le cas le plus courant en matière de services professionnels, sans imposer des réglementations très strictes en matière de télécommunications. Au Brésil par exemple, il faut un accord préalable des autorités pour le raccordement de lignes permettant de consulter des banques de données étrangères ou d'utiliser des services de traitement étrangers (cf. infra section 2). Une autre solution consiste à adopter une structure tarifaire des télécommunications qui décourage l'utilisation de services étrangers et d'encourager la croissance des services nationaux concurrents.
Pourtant, l'utilisation de services étrangers peut être très fructueuse pour un pays, notamment en tant que source d'informations scientifiques, s'il accepte la dépendance qu'elle crée et qui d'ailleurs peut n'être que temporaire.

Bien que l'application du principe du traitement national aux services télématiques présente des avantages, nous avons vu qu'il est considéré par certains pays comme dangereux pour leurs intérêts nationaux et c'est pourquoi ils lui préfèrent le principe du traitement de la nation la plus favorisée.

Ce principe est à la base du G.A.T.T., et figure dans son article premier. Il stipule que les personnes, biens ou services étrangers ne seront pas traités moins favorablement que les personnes, biens ou services de l'Etat auxquels le pays d'accueil accorde le traitement le plus favorable.
En application de ce principe, les fournisseurs étrangers de services télématiques sont tous soumis aux mêmes conditions, mais il reste possible d'accorder un traitement privilégié aux fournisseurs nationaux. Il constitue donc un compromis acceptable pour de nombreux pays tout en laissant leur marché ouvert à l'initiative étrangère.

De plus, le principe du traitement de la nation la plus favorisée admet des exceptions, par exemple pour les pays qui entretiennent entre eux des relations étroites et qui peuvent s'accorder des conditions plus favorables que celle faites aux ressortissants d'Etat tiers.

Enfin on peut rapprocher des deux principes précédents la prohibition du dumping prévue à l'article IV du G.A.T.T. et détaillée dans le Code Anti-Dumping de 1979 (12).
Ce principe interdit de proposer des biens à l'étranger à un prix inférieur à celui pratiqué sur le territoire national, et en cela contribue à créer des conditions de concurrence égales pour les nationaux et les étrangers. En effet, le dumping constitue une pratique déloyale qui porte préjudice à l'industrie nationale non seulement en l'empêchant de se développer, mais voire même en retardant sa création.

Bien que la prohibition du dumping ait été énoncée pour les biens matériels, il semble qu'elle puisse être étendue aux services télématiques du fait qu'ils occupent une part de plus en plus importante du marché, d'autant plus que la distinction entre biens et services devient de plus en plus incertaine.
En matière de télématique, on remarque surtout que les fournisseurs importants (en général américains) ont la possibilité de moduler leurs prix et risquent de ce fait d'exclure du marché les petits fournisseurs qui ne peuvent les concurrencer. L'application du principe de prohibition du dumping les protègerait contre ce genre de pratiques et maintiendrait la diversité de l'offre.

2) Le deuxième type de principes du droit international destinés à favoriser le développement des échanges commerciaux et applicables en matière de télématique sont les principes relatifs aux transports et communications (13).

Le premier d'entre eux est celui du transit libre, reconnu entre autres par la convention des Nations Unies sur le Droit de la Mer, le G.A.T.T., la Convention Postale Universelle et l'Organisation Internationale de l'Aviation Civile (I.C.A.O.). Il prévoit que lorsqu'un transport d'un pays à un autre traverse un ou plusieurs pays tiers, cette traversée doit être autorisée sans délai.
Ce principe s'applique, on le voit d'après les conventions, quel que soit le mode de transport utilisé (terre, air ou mer) et il est en conséquence logique de l'appliquer aux transferts par voie de télécommunication.
Ici encore, bien que le principe ait été formulé pour les transports de biens (marchandises, lettres,...), on peut l'étendre aux services et l'appliquer notamment aux services de transfert de données, favorisant ainsi la libre circulation de l'information.

Le principe du transit libre est susceptible d'exceptions, et notamment en ce qui concerne les transferts portant atteinte à l'ordre public (art. 19 (2) de la Convention Internationale des Télécommunications).
En matière de transfert de données, ces atteintes peuvent être constituées par exemple par des infractions au droit de la propriété intellectuelle ou à la législation protectrice de la vie privée du pays traversé, de même que par des informations sur un transfert de drogue, un détournement d'avion ou mettant en péril la sécurité nationale (14).
Ces exceptions sont cependant difficile à mettre en oeuvre, puisqu'à l'opposé des marchandises (identifiées par des documents douaniers), le contenu des transferts de données n'est pas connu des autorités nationales en application du principe du secret des correspondances.
Aussi les services télématiques bénéficient-ils actuellement d'un régime de transit libre de fait. L'affirmation du principe n'est cependant pas inutile, au cas où certains pays envisageraient d'interdire ou de restreindre le transit de données sur leur réseau national de télécommunication, entravant ainsi la libre circulation des données et le commerce international par voie de conséquence.

On peut rapprocher du principe du transit libre les principes du transit libre en douane et du débarquement libre.

Le principe du transit libre en douane est établi par l'article 24 de la Convention de l'Organisation de l'Aviation Civile Internationale (15). Afin d'éviter à un chargement transitant par plusieurs pays de passer par de multiples douanes et faciliter ainsi le commerce international, ce principe prévoit une exonération temporaire des droits de douane.
Les services télématiques professionnels, du fait qu'ils transitent sur les réseaux de télécommunication, ne sont pas soumis aux droits de douane pour des raisons pratiques. En effet, il est difficile pour les gouvernements de connaître le volume et le contenu des transferts de données à des fins de taxation sans violer le principe du secret de la correspondance.
On peut cependant penser à un régime de déclaration, bien qu'un tel régime soit facile à contourner. Toujours est-il qu'il apparait utile d'affirmer l'application du principe de transit libre en douane aux flux transfrontières de données puisqu'il est de nature à favoriser la libre circulation des données.

Le principe du débarquement libre, qui relève également du domaine de l'aviation civile (article 5 de la Convention) autorise "des arrêts brefs et nécessaires sur le territoire d'un pays survolé par un avion" (16).
En matière de flux transfrontières de données, il est fréquent que les informations soient stockées pour des raisons techniques pendant un temps plus ou moins long au cours de leur transmission dans un système informatique situé dans un pays autreque celui de destination.
En application du principe de débarquement libre, il est alors impossible aux autorités de l'Etat de transit d'avoir accès aux données temporairement stockées ou de soumettre ce stockage à des formalités quelconques (autorisation, déclaration...).

Une meilleure circulation des données, en tant que facteur de développement du commerce international et telle qu'elle est recherchée à travers l'application des principes du droit international que nous venons de voir, ne représente qu'un aspect de ce développement et doit nécessairement être accompagnée d'une amélioration de la sécurité des données transférées.

Paragraphe 2 : La protection des données

La protection des données est destinée à assurer à la fois leur sécurité (contre la perte, la destruction, la modification) et leur confidentialité (contre les accès illicites). Elle est la seconde condition indispensable au développement de l'industrie des services télématiques, puisqu'elle garantit à la fois la fiabilité du système (les données reçues sont celles qui ont été envoyées) et l'absence d'espionnage industriel et commercial. Pour les fournisseurs de services télématiques, et de banques de données en particulier, elle conserve la valeur de leur propriété.
Les mesures de protection des données sont avant tout des mesures techniques (codes, cryptographie, ...) mais il existe une protection juridique internationale dans deux cas : les données nominatives et la propriété intellectuelle. Comme pour la circulation des données, on peut dire que leur protection est à la fois un droit de l'être humain et une condition du développement du commerce international.

A. La protection des données nominatives

Le droit au respect de la vie privée est consacré par plusieurs textes du Droit International, dont les plus importants sont certainement les textes relatifs au traitement informatisé de données nominatives. Mais ce droit avait déjà été reconnu auparavant.

1) Ainsi, le droit au secret de la correspondance est considéré comme un droit fondamental de la personne humaine et figure à l'article 12 de la Déclaration Universelle des Droits de l'Homme :

> "Nul ne sera l'objet d'immixions arbitraires dans sa vie privée...son domicile ou sa correspondance..."

De même, la Convention Internationale des Télécommunications précise dans son article 22 que tous les membres "...conviennent de prendre toutes les mesures possibles qui sont compatibles avec le système de télécommunication utilisé pour assurer le secret de la correspondance internationale" (17).
Une des conséquences pratiques de ce principe est que les Etats doivent veiller à ce que leur réseau offre une sécurité suffisante et protège notamment les données contre un accès non autorisé, ce qui est d'une importance capitale pour les fournisseurs de services télématiques.

De plus, il devrait être posé clairement que le principe du secret de la correspondance s'applique également aux Etats, qui n'ont pas le droit de copier les données transmises sur leur réseau, de déchiffrer les données codées ou de s'immiscer de quelque manière que ce soit dans les communications passant par leur réseau.
Une exception pourrait cependant être admise lorsque les autorités ont de bonnes raisons de penser que les données sont susceptibles de porter atteinte à la sécurité nationale ou à l'ordre public, et à condition que cette procédure soit strictement contrôlée.

2) Dans le même ordre d'idée que le secret de la correspondance, on peut citer le principe du droit restant à l'envoyeur existant en matière de courrier classique, et qui est définit ainsi par l'article 5 de l'Union Postale Universelle (18) :

> "Tout envoi postal appartient à l'expéditeur aussi longtemps qu'il n'a pas été délivré à l'ayant-droit, sauf si ledit envoi a été saisi en application de la législation du pays de destination".

Ce principe permet aux autorités postales de déterminer à tout moment qui a le droit de disposer de biens en transit, question qui peut se révéler primordiale lorsque ces biens ont une certaine valeur. Mais évidemment, il ne définit pas qui en est le propriétaire et quelles sont ces responsabilités, questions réglées par la loi nationale applicable à la transaction.
En matière de services télématiques, les données transmises ont souvent une valeur importante mais la brièveté de leur transfert minimise la portée pratique de ce principe. On peut cependant signaler le cas où les données sont stockées pendant un certain temps au cours du processus, ce qui est fréquent dans le courrier électronique et en matière de transfert de fonds. En application du droit restant à l'envoyeur, un émetteur pourra modifier son message jusqu'au moment où celui-ci aura réellement atteint son destinataire.

3) En troisième lieu, des dispositions spécifiques à la protection de la vie privée en cas de traitement informatique des données ont été prises récemment, au niveau national et international.

En effet, nous assistons aujourd'hui au développement du traitement automatique de données personnelles, à des fins administratives et statistiques en particulier, et il en résulte un risque accru d'intrusion dans la vie privée : la

centralisation et la combinaison de données recueillies dans des buts variés permet de dresser le profil d'un individu et de prendre sur cette base des décisions quant à ses qualifications, son crédit, ... Le risque est non seulement qu'une personne non autorisée ait accès à ces données, mais également que celles-ci soient fausses, incomplètes ou irrelevantes et causent ainsi un dommage à la personne concernée (19).

De plus, au niveau international, on remarque qu'il est courant de faire traiter des données dans un pays étranger, en particulier lorsque leur propriétaire ne dispose pas des ressources informatiques nécessaires, ce qui est le cas de nombreux pays en voie de développement (P.V.D.).
Aussi de nombreux pays ont-ils adopté des dispositions législatives protégeant les données nominatives contre leur utilisation abusive, et il existe plusieurs textes internationaux ayant le même objet (Convention du Conseil de l'Europe et lignes directrices de l'O.C.D.E.). Tous ces textes ont dû résoudre deux questions : quelles sont les données sensibles? comment les protéger?

a) Quelles sont les données sensibles?

Deux approches sont ici possibles : soit énumérer les données ou les catégories de données sensibles dont la collecte doit être limitée, voire même interdite, soit considérer qu'aucune donnée n'est sensible en soi mais que n'importe laquelle peut le devenir dans certains contextes ou certaines utilisations. Plusieurs législations européennes et le projet belge ont choisi la première voie, et interdisent par exemple la collecte et le traitement de données relatives à la race ou à l'appartenance religieuse. Cette technique est cependant dangereuse, car elle laisse ouverte la possibilité qu'une donnée nominative ne soit pas comprise dans la liste et ne fasse donc pas l'objet d'une protection légale.
Aussi certains pays ont-ils préféré la seconde approche, notamment les Etats-Unis.

On a pu ensuite se demander si la protection de la vie privée s'appliquait également aux personnes morales. En effet, la législation de certains pays prévoit des restrictions aux exportations de données identifiant les personnes morales et leur reconnaissent le droit d'accès aux bases de données dans lesquelles elles figurent (corporate privacy).

Ces dispositions ont cependant été fortement critiquées, notamment en raison de leur impact néfaste sur le commerce international.

En effet, il apparaît qu'à la différence de la protection de la vie privée des personnes physiques, la motivation principale justifiant la protection de celle des sociétés est le développement de l'économie nationale du pays qui passe cette législation, puisque l'observation de ces dispositions va augmenter les coûts des importations de données (formalités administratives, ...), voire même exclure totalement la concurrence étrangère. Elles peuvent ainsi être considérées comme des obstacles non-tarifaires prohibés par le G.A.T.T. (20).

Cette question peut être perçue comme l'un des points de fiction entre une libre circulation et une protection des informations, résolu pour l'instant en faveur de la libre circulation puisqu'aucun texte international ne consacre la protection de la vie privée des personnes morales.
Mais d'un autre point de vue, on peut aussi considérer que cette solution est favorable au secret des affaires (une entreprise n'a pas accès aux fichiers d'une autre, même si elle y figure) et consacre ainsi la protection des données.

b) Comment les données sont-elles protégées?

La collecte et le traitement des données sensibles sont limités par un certain nombre de principes que l'on retrouve aussi bien dans les législations nationales que dans les textes internationaux (21) :

- le principe de limitation de la collecte : les données nominatives ne peuvent être collectées que de façon légale et honnête, et certaines données particulièrement sensibles ne peuvent pas être collectées;
- le principe de finalité : la personne qui collecte les données nominatives doit indiquer au moment de la collecte à quelles fins elles seront utilisées;
- le principe de qualité : les données récoltées doivent répondre au but poursuivi et être exactes, complètes et actuelles;
- le principe de limitation de l'utilisation : les données collectées ne peuvent être utilisées que dans le but pour lequel elles ont été collectées, sauf accord de la personne concernée ou obligation légale. Il en résulte que tout changement d'utilisation doit être signalé et autorisé, et que lorsque les données ne sont plus utiles au but poursuivi, elles doivent être détruites;
- le principe de sécurité : celui qui collecte des données doit prendre les mesures nécessaires afin qu'elles ne soient pas accessibles à des personnes non-autorisées et ne soient pas perdues, détruites, utilisées, modifiées ou divulguées;

- le principe de publicité : la personne sur laquelle portent les données doit avoir connaissance de cette collecte, ou donner son accord. De plus, chacun doit pouvoir s'informer facilement de l'existence et du contenu des fichiers de données nominatives, de leur finalité et de l'identité et de la résidence habituelle de leur propriétaire;
- le principe de participation individuelle : chacun a le droit de demander si des donnée ont été recueillies sur lui et le cas échéant, d'y accéder facilement et de les corriger ou de les annuler;
- le principe de responsabilité : l'administrateur du fichier est responsable de l'exécution des mesures prises en application des principes sus-mentionnés.

De nombreux pays, et la plupart des pays européens, ont adopté des réglementations protégeant la vie privée (22). Celles-ci suivent généralement les principes indiqués, et ne diffèrent que sur des points de détail (champ d'application, méthode de mise en oeuvre, ...).
On peut cependant signaler une distinction importante entre les pays de common law et ceux de tradition civiliste.
Dans les premiers, et en particulier l'Australie, le Canada et les Etats-Unis, les législations se contentent de reconnaître aux individus le droit d'accéder aux données nominatives détenues par les autorités administratives, alors que les législations des pays civilistes concernent également les banques de données du secteur privé. Cette divergence doit être attribuée à la différence dans l'élaboration des deux droits : alors que la common law est élaborée de façon pragmatique et ponctuelle par les cours et tribunaux, le législateur d'un pays civiliste peut imposer à tout moment des réglementations et obligations juridiques qui pèsent sur l'ensemble d'un phénomène tel qu'il peut le percevoir. Il a donc pu étendre la législation protectrice de la vie privée aux fichiers du secteur privé, même si aucune plainte ou contestation n'avait été faite contre eux.

En matière de F.T.D., on peut recenser quatre attitudes (23) :
- certaines lois ne contiennent aucune disposition spécifique applicable aux F.T.D. C'est le cas des pays anglo-saxon tels l'Australie, le Canada et les Etats-Unis;
- Au Danemark et en Allemagne, les flux transfrontières de données sont soumis aux mêmes règles que les transferts internes;
- Dans plusieurs pays, les exportations de données nominatives doivent être autorisées par une autorité spécifique (Autriche, Royaume-Uni);

- Enfin, en Israël et en Norvège une déclaration du transfert est suffisante.

Le champ d'application des législations nationales étant par nature limité au territoire du pays qui les a édicté, il a été nécessaire d'élaborer des dispositions internationales en matière de protection de la vie privée. En effet, la télématique, en facilitant les transferts électroniques de données, facilite aussi les fraudes et détournements de loi comme le prouve l'existence de "paradis de données" (dataheavens), pays où il n'existe aucune protection des données nominatives (ou une protection réduite) et qui attirent ceux qui veulent contourner les législations existantes.

Sur le plan international, le principe est que le transfert de données nominatives n'est admis que vers des pays qui offrent à ces données une protection équivalente à celle qui leur est accordée dans leur pays d'origine, et est limité, voire même interdit vers les autres pays. Ces dispositions sont mises en oeuvre par des systèmes de licence obligatoire que tout exportateur de données doit nécessairement demander et qui ne lui sera accordée que si le pays d'importation offre une protection suffisante de données.

Cette politique soulève deux difficultés.

En premier lieu, ces législations créent un obstacle à la circulation de l'information et on peut craindre qu'elles aient un effet négatif sur le commerce international en diminuant l'intérêt économique à utiliser les technologies de l'information et de la communication (24).
En effet, la grande majorité des transferts ne portent pas sur des données sensibles, mais sur des informations commerciales, culturelles, ... et l'obligation de demander une licence, si elle ne les empêche pas de circuler, ralentit indéniablement le processus et supprime un de ses principaux avantages.

La deuxième difficulté est celle de la comparaison entre le degré de protection offert par la loi du pays d'importation et du pays d'exportation. Cette recherche non seulement représente un poids supplémentaire pour les autorités chargées de la protection des données, mais de plus risque d'être longue, coûteuse et pas toujours exacte. Il est en effet à craindre que les autorités des deux pays ne soient pas d'accord quant à l'interprétation à donner à leur loi nationale.

De plus, cette politique peut aboutir à éviter certains pays dont le degré de protection n'est pas jugé suffisant, et c'est ainsi que la Grande Bretagne s'est vue obligée, sous la pression des milieux d'affaires, de passer en juillet 1984 une loi sur la protection des données sous peine de se voir exclure du circuit des transferts d'informations.

La solution à ces difficultés a été recherchée dans l'élaboration de textes internationaux destinés à dégager un consensus en matière de protection des données nominatives et à harmoniser les législations nationales. Les deux textes les plus importants aujourd'hui sont la Convention du Conseil de l'Europe et les Lignes Directrices de l'O.C.D.E.

c) La Convention du Conseil de l'Europe

Le Conseil de l'Europe a été la première organisation internationale à s'intéresser aux conséquences du progrès technologique sur la vie privée des personnes (25).
L'Assemblée Consultative demanda en 1968 au Comité des Ministres d'examiner si la Convention Européenne des Droits de l'Homme et les législations nationales des Etats-membres offraient une protection suffisante de la vie privée face au développement des nouvelles technologies. Suite à une réponse négative, ce Comité adopta en 1973 et 1974 deux résolutions établissant des critères minimum de protection des données nominatives dans les secteurs privés et publics (26).
En 1976, le Comité chargea le Comité d'Experts sur le Traitement des Données de préparer une Convention ayant pour objet la protection de la vie privée dans le traitement informatique de données, en relation avec les travaux menés à cette même époque au sein de l'O.C.D.E. et de la C.E.E.
Cette Convention a été ouverte à la signature le 28 janvier 1981 et est entrée en vigueur en octobre 1985. Elle a été ratifiée par la France, l'Allemagne, l'Espagne, la Norvège et la Suède.

Le but de cette Convention est d'assurer le respect des libertés individuelles, et en particulier de la vie privée, face au développement du traitement automatisé des données, et son préambule réaffirme l'engagement des Etats à la libre circulation des données (27).

Elle est composée de trois parties :
La première reprend les principes de base (cf. supra), en précisant qu'ils constituent un degré de protection minimum que les Etats signataires doivent assurer dans le traitement automatisé des données. Cependant, la Convention prévoit la possibilité de dérogations à ces dispositions dans un certain nombre de cas, et en particulier la non-application des principes pour certains types de données (article 3, paragraphe 2 (a)), leur extension à d'autres types de données (arti-

cle 3, paragraphe 2 (b) et (c)), et la possibilité d'appliquer des mesures de protection plus strictes que celles prévues par la Convention, sans indiquer cependant de limites sur ces points.
La seconde partie de la Convention porte sur les règles particulières aux flux transfrontières de données. Elle ne comporte qu'un article, l'article 12, qui tente de concilier les mesures de protection énoncés dans la première partie avec le principe de la libre circulation des données (Rapport explicatif, paragraphe 61).
Enfin la troisième partie prévoit une assistance mutuelle entre les Etats signataires en cas de violation de ces dispositions (article 13-7) et établit un Comité Consultatif chargé de faciliter la coopération entre les Etats (article 18-20).

En ce qui concerne les flux transfrontières de données entre les parties contractantes, l'article 12 de la Convention interdit de leur imposer des restrictions, sauf circonstances exceptionnelles : un Etat pourrait interdire ces transferts ou les soumettre à une autorisation spéciale si cette restriction n'a pas pour seul motif la protection de la vie privée. Cette disposition, destinée au départ à éviter l'utilisation de la Convention pour faire obstacle au commerce international (Rapport explicatif, paragraphe 66) risque en fait d'avoir l'effet inverse, puisque n'importe quel motif légitime autre que la protection de la vie privée justifierait de telles restrictions (28).

Le principe en matière de flux transfrontières de données est qu'ils doivent être autorisés vers les pays offrant des mesures de protection équivalentes à celles du pays d'origine des données. Il faut noter que cette condition est plus stricte que la loi nationale de la plupart des pays, qui prévoit seulement une protection "adéquate" des données dans le pays d'importation.
Lorsque des mesures équivalentes existent, les états signataires ne peuvent pas faire usage des restrictions prévues à l'article 12. Mais du fait de la possibilité de dérogation prévue à l'article 3 de la Convention (cf. supra), cette équivalence risque de n'être que rarement réalisée, justifiant ainsi l'imposition de restrictions aux transferts de données contrairement au but avoué.
En effet, dès qu'un Etat adoptera des mesures de protection plus strictes que celles prévues par la Convention en application de son article 3, il pourra interdire le transfert d'informations vers les pays ayant des dispositions plus laxistes, même s'ils sont signataires de la Convention.

Ce défaut aurait pu être évité par la définition d'un critère de protection maximum dans la Convention (29).
Une autre solution consisterait à imposer la libre circulation des données entre les pays appliquant les principes de base de la Convention. Il est cependant peu probable que les Etats signataires acceptent une telle réduction de leur contrôle sur les transferts d'informations, et c'est pourquoi l'établissement de critères maximum de protection, créant une zone dans laquelle le degré de protection est considéré comme équivalent, permettrait d'arriver à un compromis sans se référer aux législations nationales.

La Convention du Conseil de l'Europe laisse aux Etats signataires le soin de déterminer les sanctions applicables en cas de violation des lois nationales prises en application de la Convention (article 10). Ces sanctions risquent donc d'être très différentes d'un pays à l'autre pour une même infraction, et un pays pourrait considérer qu'un autre pays prévoyant des sanctions moins sévères offre un degré de protection moindre, et restreindre en conséquence les transferts vers ce pays.

En conclusion, il apparaît que cette Convention manque de cohérence, et risque en conséquence de n'avoir aucune application pratique. Aussi l'élaboration de lignes directrices était-elle peut-être plus indiquée.

d) Les lignes directrices de l'O.C.D.E.

L'O.C.D.E. a pour but de promouvoir la coopération économique entre ses Etats membres, et il est vite apparu que les divergences existant entre eux en matière de protection des données constituaient un obstacle à cette coopération.
Dès 1969, des études furent entreprises sur l'utilisation de l'ordinateur dans le secteur public, qui débouchèrent sur l'examen de la question de la protection de la vie privée et en 1978, un groupe d'experts était constitué avec pour mission d'élaborer des lignes directrices sur ce point, destinées à servir de base à une harmonisation des législations nationales des Etats membres.
Ces lignes directrices ont été adoptées par le Conseil des Ministres de l'O.C.D.E. le 23 septembre 1980 sous forme de Recommandation et ont été ratifiées par 23 états membres, dont la Belgique (manque l'Irlande).

Selon le mémorandum explicatif, les auteurs de ces lignes directrices ont cherché à maintenir l'équilibre entre le droit de l'individu au respect de sa vie privée et le principe d'une libre circulation des données "...afin de permettre une pleine exploitation de toutes les possibilités des technologies modernes de traitement de données dans des limites acceptables" (paragraphe 3).
Dans ce but, les lignes directrices énoncent un certain nombre de principes en matière de protection des données qui doivent être considérés comme des normes minimales et que les Etats membres mettent en application en les incorporant dans leur législation nationale. De cette incorporation découlera une harmonisation des lois des Etats membres et un degré uniforme de protection qui permettra une libre circulation des données entre les 24 pays membres de l'O.C.D.E. La diversité entre les lois nationales des différents pays signataires, qui est l'un des risques majeurs de la Convention du Conseil de l'Europe, n'est donc pas à craindre ici.

Les lignes directrices de l'O.C.D.E. concernent la protection des données nominatives, c'est-à-dire les informations qui se rapportent à une personne identifiée ou identifiable (article 1 (b)) qui "...en raison de la manière dont elles sont manipulées ou en raison de leur nature ou du contexte dans lequel elles sont utilisées présentent un danger pour le respect de la vie privée et des libertés individuelles" (article 2). Du fait de l'impossibilité de donner une définition des données considérées comme sensibles par tous les pays membres de l'O.C.D.E., les experts ont préféré adopter l'approche américaine qui consiste à considérer toute donnée comme potentiellement sensible (cf. supra) et ont laissé aux législateurs nationaux le soin de les définir eux-mêmes dans le cadre des principes posés par les lignes directrices (principe de qualité, de finalité, ...).

Cette protection est cependant limitée aux personnes physiques, bien que certains pays considèrent qu'elle est due également aux informations relatives aux personnes morales (Mémorandum explicatif, paragraphe 33).
Leur argument est qu'il est souvent difficile de distinguer les données personnelles des données non personnelles, en particulier dans le cas des petites entreprises, puisque les informations les concernant concernent également leur propriétaire et peuvent être de nature plus ou moins sensible.
Mais les experts ont décidé que les notions d'intégrité et de vie privée d'une personne physique étaient distinctes de l'intégrité et la sécurité d'une entreprise ou d'un groupe de personnes, et que leurs besoins de protection étaient diffé-

rents. Ils ont également repoussé la proposition de certains membres d'étendre les règles adoptées aux personnes morales et ont laissé à chaque pays le soin de décider de la protection à leur accorder.

Les données nominatives sont protégées quelque soit la manière dont elles sont manipulées, et en particulier qu'il s'agisse d'un traitement informatique ou manuel. Bien que les experts aient apporté une attention considérable au traitement automatisé des données, notamment en raison des dangers accrus que présentent pour la vie privée les technologies informatiques et le fait qu'elles soient de plus en plus utilisées, ils ont décidé de rendre ces lignes directrices applicables à tous les types de traitement et c'était la solution la plus logique.
En effet, le but de ces lignes est de protéger la vie privée, quelque soit la manière dont il y est portée atteinte et non de pénaliser les nouvelles technologies même si elles facilitent ces atteintes. Mais il faut signaler également la difficulté de distinguer entre les traitements automatisés et non-automatisés, d'autant plus qu'il existe maintenant des traitements mixtes, c'est-à-dire des traitements composés de plusieurs phases qui ne sont pas toutes informatisées. Avec le progrès technologique apparaissent de plus en plus d'équipements semi-automatisés (microfilms, micro-ordinateurs,...) qui sont utilisés par les particuliers et impossibles à contrôler. Aussi une réglementation limitée aux traitements informatisés comporterait-elle forcément des lacunes et pourrait facilement être éludée par l'application de traitements manuels aux données sensibles.

Les lignes directrices reprennent les principes mentionnés supra, et le mémorandum explicatif insiste sur le fait que ces principes sont liés entre eux, même parfois redondants (paragraphe 50) et que leur étude doit se faire de façon globale.

Les principes applicables en matière de flux transfrontières de données sont contenus dans la troisième partie des lignes directrices, constituée des articles 15 à 18 (30).
Les deux premiers ont trait à la circulation des données, et les deux autres aux restrictions qui peuvent y être apportées.

L'article 15 est relatif à la coopération entre les Etats membres en matière de protection des données nominatives, et vise en particulier à éviter que certaines données soient privées de la protection qui leur est due par la violation ou le contournement de la loi de l'un des pays membres (paragraphe 64 du mémorandum).

Cette disposition touche directement les services télématiques qui, lorsqu'ils assurent le traitement de données sensibles, devraient vérifier que ce traitement est licite aussi bien dans leur pays que dans le pays d'origine des données pour éviter d'être impliqués dans des fraudes.

L'article 16 concerne la sécurité des données transmises, et précise que les Etats membres doivent prendre les mesures nécessaires pour que les transferts soient ininterrompus et sûrs, c'est-à-dire protégés contre les accès illicites, la perte de données ou d'autres évènements du même genre (paragraphe 66 du mémorandum).
Cette disposition est à rapprocher de l'article 22 de la Convention Internationale des Télécommunications, relatif au secret de la correspondance (cf. supra). Elle implique également que cette protection doit aussi être accordée aux données en transit, c'est-à-dire aux données "...qui passent par un Etat membre sans être utilisées ou stockées afin d'être utilisées dans ce pays" (31). Cette disposition confirme l'application aux services télématiques du principe du transit libre évoqué plus haut.

Les deux articles suivants des lignes directrices concernent les restrictions qui peuvent être apportées aux flux transfrontières de données nominatives entre Etats membres.

Selon l'article 17, l'exportation des données peut être soumise à des restrictions dans trois cas :
- lorsque le pays d'importation n'observe pas "de façon substantielle" ces lignes directrices;
- lorsque cette exportation permet de contourner des dispositions législatives nationales applicables;
- lorsqu'il s'agit de données qui sont protégées de façon spécifique par la loi nationale et que les autres pays ne leur accordent pas de protection équivalente.

Selon le mémorandum explicatif (paragraphe 67), le concept de protection équivalente forme la base de l'article 17 et signifie une protection ayant "substantiellement" les mêmes effets, même si elle présente des formes différentes.
Cette définition large devrait en particulier mieux permettre d'éviter les restrictions aux exportations de données que la Convention du Conseil de l'Europe (cf. supra).

Enfin l'article 18 est un engagement des Etats à ne pas prendre des mesures en matière de protection de la vie privée qui aboutiraient à restreindre les F.T.D. au-delà de ce qui est nécessaire.

Si ces lignes directrices constituent un premier pas appréciable vers l'harmonisation des législations nationales, elles ne lient pas les Etats et sont seulement une invitation à appliquer les principes énoncés (32).

Les services télématiques doivent veiller à respecter les dispositions protectrices de la vie privée, aussi bien au niveau national qu'international. En effet d'un point de vue pratique, ces dispositions touchent un certain nombre de F.T.D. Elles s'appliquent ainsi aux transferts de données médicales, financières, aux transferts de listes de clients, de fournisseurs, de personnel...

Le second type de données protégées au niveau international sont celles qui font l'objet d'un droit de propriété reconnu juridiquement.

B. La protection de la propriété intellectuelle

Les services télématiques professionnels sont intéressés par la protection de la propriété intellectuelle au niveau international à deux titres : pour protéger leur propre bien, c'est-à-dire les logiciels et la banque de données, et pour protéger les droits des auteurs dont les oeuvres sont reprises dans la banque de données (cf. supra). Il existe en matière de droits d'auteur deux accords internationaux, la Convention de Berne du 9 octobre 1886 et la Convention de Genève du 6 septembre 1952. Mais même si l'auteur est ressortissant de l'un des très rares pays qui n'ont adhéré à aucune des deux conventions, les législations nationales prévoient des dispositions protectrices à son égard.

a) La Convention de Berne

Signée le 9 octobre 1886 à Berne, cette Convention a été révisée plusieurs fois depuis et la version actuelle est celle qui a été adoptée à Paris en 1971. Elle a été signée par 76 Etats au 1er janvier 1986 et son siège est à Genève, où elle est gérée par l'Organisation Mondiale de la Propriété Intellectuelle. Cette convention retient deux principes : l'assimilation de l'auteur étranger à un auteur national et l'établissement d'un degré minimum de protection (33).

Selon l'article 5-1 de la Convention "...les auteurs jouissent, en ce qui concerne les oeuvres pour lesquelles ils sont protégés en vertu de la présente Convention, dans les pays de l'Union autres que le pays d'origine de l'oeuvre, des droits que les lois respectives accordent actuellement ou accorderont par la suite aux nationaux, ainsi que des droits spécialement accordés par la présente Convention".

Les oeuvres protégées par la Convention sont détaillées dans son article 2, qui vise "toutes les productions du domaine littéraire, scientifique et artistique quelqu'en soit le mode ou la forme d'expression".
Le second paragraphe de cet article prévoit la possibilité pour les Etats signataires de ne pas protéger les oeuvres qui ne sont pas fixées sur un support matériel, mais les programmes et les données sont nécessairement enregistrés sur un support magnétique (disque ou bande) et cette disposition ne devrait donc pas s'appliquer aux services télématiques.

Enfin, le paragraphe 5 de l'article 2 prévoit la protection des oeuvres secondes (anthologies, encyclopédies, ...) et on peut donc considérer que la Convention de Berne est applicable aux banques de données, en conformité avec le raisonnement suivi par la Cour de Cassation française dans l'arrêt Microfor-Le Monde.

La protection de la Convention de Berne s'applique aux auteurs ayant la nationalité d'un des Etats signataires (ou sa résidence habituelle dans un tel Etat) pour les oeuvres publiées ou non et à tout autre auteur pour les oeuvres publiées pour la première fois dans un des pays membres (même si une publication simultanée a lieu dans un ou plusieurs pays non membres) (article 3).

La publication est l'édition d'une oeuvre avec le consentement de son auteur "...quel que soit le mode de fabrication des exemplaires pourvu que la mise à disposition de ces derniers ait été telle qu'elle satisfasse les besoins raisonnables du public compte tenu de la nature de l'oeuvre" (article 3, paragraphe 3).
On peut donc estimer que l'enregistrement sur support magnétique correspond à la définition d'une publication et doit être autorisé par l'auteur. Cette conclusion est confirmée par les articles 11, 11bis et 11ter de la Convention, selon lesquels les auteurs jouissent du droit exclusif d'autoriser la communication publique de leur oeuvre par tous moyens (représentation, radiodiffusion, récitation, ...) et par l'article 9, paragraphe 3 selon lequel tout enregistrement sonore ou visuel est considéré comme une reproduction.

La protection accordée par la Convention consiste en un monopole d'exploitation reconnu à l'auteur, qui a seul le droit d'autoriser la traduction (article 8), la reproduction (article 9), la représentation (article 11) et l'adaptation de son oeuvre (article 12). Elle comprend également le droit moral pour l'auteur de revendiquer la paternité de son oeuvre et de s'opposer à toute modification de celle-ci même après la cession de ses droits (article 6bis, paragraphe 1). Cette disposition permettrait en particulier à un auteur d'intenter une action contre le producteur de banque de données qui aurait déformé son oeuvre.

b) La Convention de Genève

Conclue le 6 septembre 1952 sous l'égide de l'U.N.E.S.C.O. et révisée lors de la Conférence de Paris en 1971, cette Convention groupe les pays qui considèrent la Convention de Berne comme trop protectrice des auteurs et préfèrent en conséquence s'abstenir de la ratifier. Elle comprenait le 1er janvier 1976 69 pays membres, dont les Etats-Unis et l'U.R.S.S.
Du fait que cette Convention est moins protectrice, il était à craindre que plusieurs pays ne quittent la Convention de Berne et c'est pourquoi deux mesures de sauvegarde ont été prises : l'interdiction de quitter la Convention de Berne pour adhérer à la Convention de Genève à partir du 1er janvier 1951 et l'obligation de l'appliquer dans les relations entre deux de ses états membres même s'ils ont adhéré à la Convention de Genève (article 17). Depuis 1971 cependant, cette clause ne joue plus dans les rapports entre les pays développés et les P.V.D. qui quittent la Convention de Berne (34).

Les principes retenus par la Convention de Genève sont à peu près les mêmes que ceux vus précédemment (protection des oeuvres littéraires, scientifiques ou artistiques de toute sorte, assimilation des auteurs étrangers ressortissant ou domiciliés dans un autre état membre aux auteurs nationaux et protection de la première publication d'un auteur tiers si elle a lieu dans un pays membre).
La notion de publication est cependant plus étroite ici que dans la Convention de Berne, puisqu'elle signifie la mise à la disposition du public sous une forme lui permettant de lire l'oeuvre ou d'en prendre connaissance visuellement (article 6). Cette limitation ne touche cependant pas les services télématiques qui sont toujours fournis sous une forme visuelle, que ce soit sur l'écran du terminal ou sur le papier de l'imprimante.

Les droits reconnus à l'auteur par la Convention de Genève sont moins nombreux que dans la Convention de Berne. En 1952, seul le droit exclusif de traduction était consacré (article 5).
La version révisée de 1971 reconnait le droit exclusif de l'auteur d'autoriser la reproduction par n'importe quel moyen, la représentation, la radiodiffusion et l'adaptation (article 4bis), mais laisse aux Etats membres la possibilité d'apporter des dérogations à ces droits à condition qu'ils accordent "...un niveau raisonnable de protection effective".

En matière de services télématiques, les droits les plus importants pour les auteurs sont le droit de reproduction et de représentation et il apparaît donc que la Convention de Genève ne les protège pas directement, mais que cela dépend de la politique nationale du pays ou les actes critiqués (reproduction illicite essentiellement) auront eut lieu. Au niveau international, la Convention de Berne leur accorde une protection plus adéquate mais évidemment limitée à ses pays membres.
Or nous avons vu qu'en matière télématique il est facile d'avoir accès à des services situés à l'étranger. Les services professionnels faisant toujours l'objet, du moins actuellement, de contrats préalables, on peut estimerque le fournisseur de services télématiques qui aurait des doutes sur le respect de ses droits dans un pays déterminé pourrait refuser de servir un client établi dans ce pays ou prévoir des dispositions contractuelles spécifiques (en particulier quant à la loi applicable et au tribunal compétent).

c) Les législations nationales

Enfin les législations nationales contiennent généralement des dispositions relatives à la protection des oeuvres d'auteurs étrangers sur leur territoire. Ainsi, l'article 38 de la loi belge du 22 mars 1886 reconnaît aux étrangers les mêmes droits que les auteurs nationaux, en l'assortissant cependant d'une condition de réciprocité : si les auteurs belges jouissent d'une protection moindre dans un pays déterminé, les droits des ressortissants de ce pays sur les oeuvres publiées en Belgique seront restreints dans les mêmes limites.
En France également, les articles 70 et 71 du Code Pénal reconnaissent l'égalité de traitement entre les oeuvres nationales et étrangères, et les droits d'auteur ont pendant longtemps été considérés comme des droits civils, dont les étrangers peuvent jouir en France sans condition de réciprocité.

Cependant, face au refus de certains Etats étrangers d'adhérer aux Conventions internationales en la matière et de protéger les oeuvres des auteurs étrangers, la loi du 8 juillet 1964 a imposé une conditions de réciprocité à cette protection.

Enfin, l'amélioration au niveau international de la circulation et de la protection des données transmises sur les réseaux télématiques passe par une condition plus pratique que juridique : la normalisation des pratiques dans ce domaine, c'est-à-dire leur harmonisation au niveau international afin d'améliorer leur efficacité tout en réduisant leur coût.

Paragraphe 3 : La normalisation

On distingue la normalisation technique de la normalisation administrative.

A. La normalisation technique

> "Le premier pas vers une réglementation générale et internationale dans un domaine est bien souvent la réglementation de ses aspects techniques. C'est une approche commode puisque les problèmes politiques ne sont peut être pas aussi prédominants dans les domaines techniques que dans d'autres domaines plus substantiels" (35).

Cette constatation s'applique aussi aux services télématiques internationaux.

La normalisation des équipements de transmission de données (ordinateur + réseau) consiste à édicter des normes et standards auxquels ces équipements doivent obéir pour être compatibles entre eux. Elle facilite la diffusion des services télématiques en leur permettant d'emprunter les réseaux de fournisseurs différents, ce qui est particulièrement utile sur le plan international où la diversité des équipements est très marquée.
La normalisation favorise également la concurrence sur le marché des services et équipements, puisque les utilisateurs ne sont pas obligés de se limiter à une seule marque et que de nouveaux fournisseurs peuvent se lancer sur le marché sans craindre la position dominante de quelques uns.

Il faut cependant noter que la normalisation accroit la vulnérabilité d'un Etat, puisqu'elle permet à des éléments extérieurs d'intervenir plus facilement sur le réseau de télécommunication de cet Etat.

Au niveau international, la nécessité d'une normalisation technique en matière de télécommunication est reconnue depuis longtemps, et elle est à la base de la Convention Internationale des Télécommunications (article 4.1.c).
Elle est entreprise actuellement par des organismes internationaux tels que l'I.S.O. (International Standard Organization) et le C.C.I.T.T. (Comité Consultatif International pour le Télégraphe et le Téléphone) (36).
On peut citer comme exemple des normes existantes le Code A.S.C.I.I. (American Standard Code for Information Interchange) applicable au codage des informations et la norme V24 du C.C.I.T.T. relative à la connexion au modem pour la transmission de données.

Etant admis que le principe d'une normalisation est souhaitable, la question se pose de la stratégie à adopter dans ce domaine pour l'avenir, et en particulier quant à l'autorité compétente pour édicter ces normes : les Etats? des organismes para-étatiques? des organisations privées, comme c'est le plus souvent le cas aujourd'hui? (37).

En matière de télécommunication, le gouvernement a souvent un rôle de normalisation de fait au niveau national puisque nous avons vu que le réseau est dans de nombreux pays un monopole d'Etat. Celui-ci peut exercer sa fonction normative de trois manières : soit en conservant le monopole de fourniture de l'équipement technique, soit en contrôlant cet équipement par une procédure d'agrément qui en assure la compatibilité au niveau national, soit enfin en adoptant une formule mixte, telle qu'elle existe en Belgique, dans laquelle les matériels au delà d'une certaine puissance peuvent être fournis par des entreprises privées ayant obtenu un agrément des autorités.

Au niveau international, on peut penser à trois solutions.

La première consisterait en l'adoption d'un texte international par les Etats imposant directement les normes applicables. Bien qu'elle permette un contrôle efficace de leur application, cette solution apparaît cependant comme inappropriée. En effet, l'élaboration d'un texte de ce genre va se révéler longue et difficile, compte tenu de l'étendue du domaine à normaliser, et risque en plus d'engendrer une rigidité peu souhaitable dans un domaine où la technologie est en rapide évolution.

Une seconde solution consisterait à définir, dans un texte international, les normes généralement utilisées en matière de transfert de données, à l'exemple de ce qui existe déjà en matière de Commerce International avec les Incoterms de la Chambre de Commerce Internationale.
Dans leurs transactions, les parties choisiraient les modalités de l'opération parmi celles proposées par la Convention. Tout en introduisant des normes uniformes et en clarifiant les responsabilités des parties, cette solution présente l'avantage de conserver la souplesse nécessaire à l'adaptation des normes au progrès technologique.

Enfin la dernière solution consisterait à établir des normes techniques au niveau international directement. C'est la solution généralement adoptée lorsque la nécessité de telles normes devient pressante et que le nombre d'experts capables de les formuler est réduit. Ainsi les normes en matière de télécommunication ont-elles été édictées directement par des organisations professionnelles concernées.

Dans la Communauté Européenne, on note que les normes et réglementations techniques sont décidées au niveau national. Elles sont cependant contrôlées par la Commission afin d'atténuer les inconvénients éventuels qu'elles pourraient avoir sur la libre circulation des produits et de promouvoir une uniformisation des normes au niveau européen (38).

Deux autres questions restent à résoudre en matière de normalisation : quelle est la force obligatoire des normes? Quel est leur contenu?
La force obligatoire des normes dérive seulement pour l'instant de l'intérêt privé du constructeur à conserver sa place sur le marché. Seul un constructeur très puissant pourrait imposer ses propres normes, mais on constate alors que ce sont ceux-là qui font partie et dirigent les organisations professionnelles édictant les normes.
Sur le second point, le contenu des normes, on peut se demander si la normalisation ne doit porter que sur les caractéristiques externes des équipements (leur compatibilité, leurs fonctions) ou également sur leurs mécanismes internes. Cette deuxième solution résulterait en une pression plus forte sur les constructeurs qui, on peut le craindre, entraverait les innovations technologiques (cf. en ce sens la "transaction" IBM - CEE d'octobre 1984).

Enfin la normalisation technique internationale risque de poser un problème de coût, spécialement pour les pays les moins avancés. En effet, les normes préconisées sont souvent

celles des matériels les mieux développés, qui sont en général relativement chers. La conformité de leur matériel avec les normes internationales entrainerait des investissements trop lourds pour certains pays, et c'est pourquoi M. BING propose d'établir un schéma de classification des réseaux de communication selon le degré d'avancement de la technologie qu'ils utilisent (39). Ce schéma présenterait l'avantage de fournir des indications sur les spécifications techniques des réseaux des différents pays, sans incidence sur l'économie de ceux-ci. Il pourrait même les encourager à modifier les caractéristiques techniques de leurs réseaux afin de rendre leurs entreprises nationales plus présentes sur le marché international.

On peut enfin rapprocher du principe de la normalisation de l'équipement technique le principe de qualité technique prévu par certaines conventions, et selon lequel les pays doivent veiller à la haute qualité technique de leur réseau de communication (vitesse élevée, absence de perturbations, ...), par exemple l'article 23 de la Convention Internationale des Télécommunications et l'article 6 de la Convention sur le régime international des chemins de fer.

B. La normalisation administrative

A côté de la normalisation technique, la normalisation administrative consiste en l'harmonisation des pratiques suivies, des documents utilisés, des procédures administratives afin de promouvoir une meilleure circulation "juridique" des données.

Une telle normalisation présenterait en particulier des avantages réels en matière commerciale. A plus long terme, elle permettrait l'élaboration de documents internationaux reconnus comme authentiques par les différents pays (par exemple en matière de transferts électroniques de fonds; voir aussi le Data Freight Receipt en matière de transports maritimes).
A propos des T.E.F., M. WYMEERSCH écrivait :

> "Le domaine des opérations télématiques financières semble être également propice au développement de règles professionnelles, à la standardisation des opérations et à l'application d'usages divers, qui ont ceci de commun, qu'ils émanent, non pas d'une source de droit étatique, mais de conventions privées, de décisions d'une association, voire même de l'assimilation de la règle par un milieu déterminé. Le phénomène se manifeste sur le plan national, et peut-être avec plus de vigueur sur le plan international".

A propos de la normalisation administrative comme pour la normalisation technique se poseront les questions des "auteurs" de la norme, de sa valeur obligatoire, de ses sanctions et des effets anti-concurrentiels que peut entraîner l'application majoritaire de normes.

L'un des principaux arguments contre la normalisation est la vulnérabilité du réseau qu'elle engendre. Aussi les efforts de normalisation ont-ils également porté sur la sécurité. La normalisation administrative porte en effet sur l'obligation pour chaque participant à l'opération, de suivre certaines règles de sécurité tant dans la procédure d'établissement des documents que dans son environnement (déontologie du personnel, nomination de responsables, etc.).

Les services télématiques sont les premiers bénéficiaires de la normalisation, tant technique qu'administrative et il n'est donc pas étonnant de constater qu'ils se trouvent parmi ses promoteurs.

Ayant ainsi établit une liste des principes du droit international qui trouveraient à s'appliquer aux services télématiques, nous devons voir ce qu'il en est en pratique. En effet, la force exécutoire de principes internationaux est subordonnée à leur application au niveau national, et c'est pourquoi nous avons consacré la deuxième section de ce chapitre à la façon dont les différents Etats appréhendent les flux transfrontières de données en général, et les services télématiques en particulier.

SECTION 2 - La mise en oeuvre au niveau national

D'un point de vue général, on peut dire que l'amélioration de la circulation des données entrainée par les nouvelles technologies présente des avantages à la fois pour les pays développés et ceux en développement.

Les pays développés y trouvent à la fois une opportunité d'exporter leur matériel sophistiqué (ce qui est favorable à leur économie) et une façon de communiquer facilementavec leurs filiales situées à l'étranger et d'améliorer ainsi la conduite des affaires (ce qui a également un effet positif sur les bénéfices).

Pour les pays en développement, une meilleure circulation des données signifie à la fois une amélioration de leur accès aux technologies de pointe et par là un facteur de développement,

et la possibilité de profiter de ces nouvelles technologies à moindre coût, puisqu'en utilisant la télématique ils peuvent profiter des ressources informatiques dont ils ne disposent pas. Ces pays sont cependant réticents aux flux transfrontières de données, en particulier pour des raisons de souveraineté (40).

Paragraphe 1 : La protection de la souveraineté

La libre circulation des données est perçue par de nombreux Etats, en particulier dans les P.V.D., comme une menace pour leur souveraineté et leur indépendance. Ainsi, on remarque que le motif le plus souvent invoqué pour refuser l'application de certaines dispositions des conventions internationales est la sécurité nationale (qui est d'ailleurs reconnue comme une exception par la plupart d'entre elles).

Le recours à des services télématiques étrangers présente effectivement des dangers, parmi lesquels on peut citer :
- la perte de contrôle sur les données une fois qu'elles quittent le territoire national en raison de la territorialité des lois; elles peuvent ainsi non seulement perdre la protection à laquelle elles ont droit, mais également être utilisées à des fins illicites dans leur pays d'origine;
- la dépendance vis-à-vis des Etats vers lesquels les données sont exportées pour être traitées ou stockées.
Pour prendre les décisions, les dirigeants d'un pays, autant au niveau public que privé, ont besoin d'avoir accès à l'information. Si celle-ci est stockée à l'étranger, l'Etat devient vulnérable du fait qu'il existe toujours le risque qu'elle soit retenue dans ce pays (par analogie avec le gel des avoirs iraniens aux Etats-Unis) ou faussée intentionnellement.
De plus, le stockage de données à l'étranger risque d'empêcher un Etat de fournir à ses ressortissants les services administratifs auxquels ils ont droit;
- l'atteinte à la vie privée de ses ressortissants par le contournement des dispositions nationales applicables et le traitement des données nominatives dans des pays qui ne sont pas signataires des accords internationaux dans ce domaine; et enfin
- l'atteinte à l'économie nationale, en particulier du fait que les services étrangers étant faciles à utiliser, ils constituent un obstacle pour le développement de l'industrie informatique locale et en conséquence de l'emploi.

Ces dangers sont réels, et justifient certainement la prise de mesures destinées à les contrer. Il est cependant à craindre que celles-ci ne paralysent la circulation des données au-delà de ce qui est souhaitable, et c'est pourquoi on admet généralement que leur effet général doit être limité au strict nécessaire (41).

En second lieu, il apparaît que le concept de souveraineté subit aujourd'hui une transformation : La souveraineté n'est plus seulement une question de frontières territoriales ou d'allégeance politique, mais également "...la facilité d'accéder à des ressources en matière d'information, d'exercer le contrôle sur ces ressources et de les exploiter", qui constituerait une "souveraineté informationnelle" (42).

On voit ainsi s'affronter deux conceptions des flux transfrontières de données au niveau international :

Pour certains pays, ces flux constituent une menace pour leur souveraineté et leur indépendance, ce qui les amène à édicter des réglementations restrictives dans ce domaine.
Il s'agit généralement de pays en développement (Brésil en particulier), mais pas nécessairement. Ainsi au Canada, le Comité Consultatif du Département des Communications, chargé d'une étude sur les implications des télécommunications sur la souveraineté canadienne, (43) a recommandé au gouvernement de réglementer les flux transfrontières de données "...pour assurer que nous ne perdions pas le contrôle d'informations vitales pour le maintien de la souveraineté nationale" (Recommandation 24).

La seconde attitude est celle des pays qui considèrent que ces réglementations constituent des restrictions au Commerce International interdites par le G.A.T.T. C'est essentiellement la position des Etats-Unis (44).
Jusqu'à présent, on doit constater que les réglementations nationales restreignant les flux transfrontières de données continuent à constituer des obstacles à la libre circulation recommandée par le droit international et par là au développement des services télématiques.

Paragraphe 2 : Les réglementations nationales

La première réglementation nationale qui touche les services télématiques est la réglementation des télécommunications (45). Nous avons vu (cf. supra chapitre I) que de nombreux pays ont établi un monopole étatique sur le réseau qui fait obstacle à ce que des services privés de télécommunication, qu'ils soient nationaux ou étrangers, puissent être proposés alors qu'ils sont souvent plus performants.

D'un point de vue technique, la normalisation recommandée par la Convention Internationale des Télécommunications (cf. supra) est en bonne voie et il faut reconnaître qu'il n'est pas trop difficile de transférer des données à l'étranger en passant par les réseaux nationaux, tout en tenant compte cependant de l'insécurité et de l'absence de garanties sur ces réseaux, et de la nécessité de vérifier la compatibilité des équipements informatiques qui, elle, est loin d' être réalisée.

En second lieu, les réglementations nationales destinées à protéger les données nominatives et la propriété intellectuelle contiennent également des dispositions relatives à la diffusion à l'étranger de ces données ou à la protection sur le territoire national de données étrangères (protection des auteurs étrangers). Du fait de l'existence de textes internationaux dans ce domaine et de leur ratification par la majorité des Etats, les principes appliqués au niveau national sont ceux étudiés précédemment : traitement national, notion de protection équivalente et condition de réciprocité.

Deux autres types de réglementations seront étudiées plus en détail : les réglementations spécifiques à l'informatique ou la télématique et les dispositions fiscales et douanières.

A. Les réglementations de l'informatique

Soixante pays environ ont adopté des dispositions spécifiques à l'informatique, relatives le plus souvent à l'acquisition de matériel de traitement et définissant des priorités pour leur utilisation, ou suivent une politique dans ce sens (46). Ces dispositions ont par voie de conséquence un effet sur les services télématiques et sur les F.T.D. Mais certains pays ont même élaboré des politiques spécifiques aux flux transfrontières de données non personnelles. Parmi eux, on peut citer le Canada, la Suède, la France, le Brésil et les Communautés Européennes (47).

La législation brésilienne est souvent citée comme l'exemple le plus marquant de régulation des F.T.D., à la fois par la clarté de ses motifs et sa sévérité, mais elle ne doit pas masquer le fait que plusieurs pays ont déjà élaboré ou envisagent d'élaborer des législations dans ce sens. A titre d'illustration, nous analyserons rapidement deux législations représentatives, celles du Brésil et du Canada (48).

a) La législation brésilienne

En ce qui concerne les services télématiques, la politique du Brésil est très claire : "le gouvernement du Brésil ne permet pas l'utilisation d'ordinateurs situés à l'étranger qui, par la télématique, accomplissent des tâches dont la solution peut être obtenue dans le pays" (49).

Son but avoué est de promouvoir la création et le développement d'une industrie nationale en matière d'informatique et de télématique par un protectionisme exacerbé (exclusion systématique de la concurrence étrangère, augmentation des participations de l'Etat et établissement de normes favorables aux produits nationaux).

En 1972 était créée la Commission pour la Coordination des Activités de Traitement Informatique (C.A.P.R.E.) au Ministère du Plan, chargée de surveiller l'acquisition et l'utilisation d'ordinateurs, au début seulement au sein du Gouvernement Fédéral, puis à partir de 1976 pour tout ordinateur ou équipement informatique.
En mai 1978, une loi élaborée à la demande du Ministère des Télécommunications et sur proposition de la C.A.P.R.E. instaurait un régime d'accord préalable pour l'utilisation de systèmes télématiques au niveau international.
En application de cette loi, la C.A.P.R.E. analysait les demandes en considérant leur effet micro- et macro-économique ainsi que de leur effet sur la vie privée et la souveraineté et donnait un accord valable 3 ans au maximum.
Entre le 1er mai 1978 et janvier 1980, 16 décisions ont été prises : l'accord a été donné à des systèmes de réservation de places d'avion et à des systèmes de démonstration.
Il a par contre été refusé pour l'utilisation de services télématiques étrangers (services de traitement et banques de données) et certaines opérations inter-entreprises.

Au début 1979, une nouvelle loi créait le Secrétariat Spécial à l'Informatique (S.E.I.), successeur de la C.A.P.R.E., et renforçait et élargissait ses attributions.
En 1980, la Commission Spéciale pour la Télématique créée par le S.E.I. remettait un rapport approuvant la procédure de l'accord préalable pour le raccordement de lignes permettant de consulter les banques de données étrangères.
Les renseignements à fournir pour obtenir cet accord sont extrêmement détaillés, et insistent particulièrement sur l'absence d'équipement semblable sur place et le bénéfice que tirera le Brésil de l'opération.

Jusqu'à présent, aucun accord n'a encore été donné pour l'utilisation de services de traitement étrangers, apparamment en raison de l'incertitude du gouvernement brésilien quant aux conséquences sociales et économiques qui s'ensuivraient (50).

b) La réglementation canadienne

Si la Recommandation 24 du Comité Consultatif du Département des Communications canadien n'a jamais été officiellement acceptée par le Gouvernement, les réglementations de certains types d'investissements étrangers reflètent l'attention qu'il apporte aux F.T.D. et à la protection de la souveraineté canadienne (51).

Ainsi le "Foreign Investment Review Act" de 1974 a instauré un contrôle des investissements étrangers du Canada. Selon le milieu des affaires, cette loi aurait été appliquée de façon particulièrement stricte aux investissements étrangers dans l'industrie canadienne de services informatiques.

Le cas de la société américaine Comshare est particulièrement illustratif de cette tendance. Cette société, actionnaire minoritaire de la société C.S.L., société canadienne de services informatiques, souhaitait acquérir un certain nombre d'actions afin de devenir majoritaire.
Afin d'obtenir l'accord nécessaire, Comshare avait donné de nombreux renseignements sur ses activités et ses finances aux autorités canadiennes et avait accepté de les avertir par écrit de toute modification ou réorganisation. Elle s'était également engagée à suivre un programme d'expansion favorable à l'économie canadienne (investissements supplémentaires au Canada, formation de canadiens, transferts de technologie et exportation de services informatiques vers l'étranger).
Malgré ces engagements, la demande fut rejetée du motif que l'opération n'apportait pas un bénéfice suffisant pour le Canada.

Un autre exemple de cette tendance est fourni par la révision de 1980 de la loi sur les banques et les activités bancaires (Banks and Banking Law Revision).
Cette révision autorise pour la première fois les banques étrangères à ouvrir une filiale au Canada directement (sans passer par une banque locale). Comme les banques sont l'un des plus grands utilisateurs de la télématique, cette mesure devait nécessairement entraîner un accroissement des F.T.D. et du traitement et du stockage de données à l'étranger, et notamment aux Etats-Unis. Aussi la loi a-t-elle prévu cette situation et oblige-t-elle à conserver au Canada certains types de dossiers de clients (53).

De plus, les banques doivent conserver sur place, sous forme de papier, de film ou sous forme électronique tous les dossiers et registres requis par la loi bancaire, et si la forme électronique est choisie, la banque doit stocker les données au Canada et disposer sur place de l'équipement nécessaire pour reproduire toute information sous forme écrite et lisible dans un délai raisonnable.

Enfin, la loi admet que certains traitements informatiques peuvent être exécutés à l'extérieur du Canada à condition toutefois d'en informer l'Inspecteur des Banques (qui peut l'interdire), et de lui fournir une description des documents envoyés et du traitement appliqué.
Le Ministre des Finances lui-même peut interdire un tel traitement lorsqu'il s'avère être contraire à l'intérêt national.
Si le pouvoir reconnu à l'Inspecteur des Banques est motivé par la nécessité d'avoir accès à ces documents pour accomplir sa mission de contrôle, l'intervention du Ministre des Finances apparaît clairement comme une façon de réglementer les F.T.D. entre banques.

En conclusion de ce point, on remarque que les dispositions nationales ayant spécifiquement pour objet de restreindre les flux transfrontières de données sont motivées, soit par la protection de l'industrie nationale, soit par le maintien d'un contrôle de l'Etat sur les activités traditionnellement soumises à un tel contrôle et qui pourraient, par l'utilisation des nouvelles technologies, y échapper. Ces dispositions illustrent l'érosion de la souveraineté qu'entraîne la télématique, et que confirme la recherche de la loi applicable. Mais avant de passer à ce point, il est apparu intéressant de consacrer quelque développement aux aspects douaniers et fiscaux de la télématique.

B. Les réglementations douanières et fiscales

Au fur et à mesure que les transferts d'information grandissent en importance, il est tentant pour les gouvernements d'en faire une source de revenus supplémentaires.
Au niveau national, il est à craindre que l'imposition de ces transferts les rendent plus chers, donc moins compétitifs sur le marché international et entrave par là leur développement.
Mais l'idée d'une taxation des transferts internationaux d'information a paru plus séduisante à certains, qui ont proposé d'appliquer aux F.T.D. les mêmes principes de taxation que ceux appliqués aux transferts de marchandises (54).

En effet, cette taxation non seulement procurerait des revenus supplémentaires à l'Etat, mais constituerait également une protection de l'industrie nationale de l'information en rendant plus onéreuse la pénétration du marché pour les entreprises étrangères.

Mais pour pouvoir taxer les flux transfrontières de données, il faut pouvoir les appréhender.
Ainsi la réglementation douanière s'applique à tous les flux transfrontières de marchandises, c'est-à-dire de choses "...susceptibles d'appropriation individuelle et de transmission" (Cass. Crim. Française, 17-10-1967), même si elles ne sont pas nécessairement l'objet d'échanges marchands.
Les colis familiaux par exemple sont également soumis aux formalités douanières.
Par contre ces choses doivent nécessairement avoir un caractère matériel. Les biens incorporels franchissant les frontières ne sont pas appréhendés, à l'exception de l'énergie électrique qualifiée de "meuble par nature".

En ce qui concerne les flux d'informations, les Douanes ne les appréhendent que lorsqu'ils sont matérialisés sur un support (imprimé, bande ou disque magnétique, films...), puisqu'elles n'ont pas connaissance des informations transitant par câble ou ondes magnétiques.
De plus, en matière télématique, ces transferts s'effectuent tous sous forme de "bits" informatiques et il est impossible de distinguer les différentes sortes de transferts s'ils sont soumis à des régimes de taxation divers.

Enfin, si les Douanes parviennent tout de même à appréhender ces flux (par des régimes de déclaration obligatoire par exemple), il faudra résoudre la question de la méthode de calcul par leur imposition.
Lorsque les informations sont achetées ou les services fournis par des tiers, ils donnent lieu à un prix qui peut servir de base à l'impôt. Mais la majorité des transferts se font à l'intérieur des entreprises multinationales et ne donnent pas lieu à un paiement. Il faudrait donc procéder à une estimation de leur prix ou de leur valeur pour pouvoir les taxer, ce qui serait très difficile à mettre en pratique (55).

Pour calculer la valeur des flux d'informations matérialisés, les Douanes additionnent la valeur du support (élément matériel) et la valeur de l'information qu'il contient (élément intellectuel). Avant le 1er juillet 1980, cette

valeur était calculée en ajoutant au prix du support un pourcentage forfaitaire correspondant aux frais de rédaction et/ou d'enregistrement, et donc pas à la valeur de l'information elle-même.
Depuis le 1er juillet 1980, date d'entrée en vigueur du règlement C.E.E. 1224/80 du Conseil daté du 25 Mai 1980 pris et en application de l'article 7 de l'accord du G.A.T.T.de 1979, toutes les marchandises doivent être évaluées sur base de leur valeur transactionnelle, ou par recours à cinq méthodes de substitution en cas d'absence ou de contestation de cette valeur.

En matière télématique, on a objecté que des données ou des programmes transmis par câble ou par satellite ne sont pas taxables en douane, alors qu'ils le deviennent s'ils sont transmis sur un support matériel. Aussi le Comité de l'Evaluation du G.A.T.T. a-t-il décidé, le 24 septembre 1984, de reconnaître un régime particulier pour les supports informatiques, applicable facultativement par les pays membres du G.A.T.T. Selon cette décision, les transferts informatiques seront évalués en douane sur la valeur du support seul, sauf s'il s'agit d'un circuit intégré, d'un semi-conducteur, d'un composant similaire ou d'un article comportant de tels circuits ou composants, ou d'enregistrements sonores, cinématographiques ou vidéo.

En pratique, les Douanes ne prennent pas en compte la valeur de l'information à condition qu'elle puisse être distinguée de la valeur de son support, sur la facture ou le contrat de vente par exemple.

Cette Recommandation du G.A.T.T. a été ratifiée par la C.E.E. en Avril 1985 (Décision du Conseil n. 1055/85). On peut déduire de ces dispositions que les transferts télématiques de données, du fait qu'ils ne sont pas incorporés dans un support matériel, sont exonérés de droits de douane.
La possibilité reste cependant ouverte de les assimiler à des meubles par nature, par analogie avec l'électricité. Mais cette assimilation risque de poser des problèmes d'évaluation : l'électricité à une valeur uniforme, alors que la valeur de l'information varie selon son contenu.

En ce qui concerne la T.V.A., on distingue les importations avec ou sans support.
Dans le cas des importations sur support, la base d'imposition est définie par la législation douanière nationale, et dans la C.E.E. conformément aux règlements communautaires en vigueur.Mais les importations d'information sans support sont considérées comme des prestations de service, qui échappent à la T.V.A. à l'importation. Elles sont par contre soumises à la T.V.A. en régime intérieur, toujours à condition de pouvoir les appréhender.

Cette réflexion nous amène à la pratique comptable. Sur ce point, on remarque que les transferts de données n'ont pas de statut établi et que les entreprises suivent des pratiques variées.
En général, elles ne comptabilisent pas les envois de messages. De même, les échanges de données entre firmes liées (mère et filiales) sont rarement facturées et comptabilisées. Mais même lorsque ces transferts sont comptabilisés, on ne sait pas s'ils peuvent être considérés comme des "charges" (déductibles fiscalement) et il n'existe aucun contrôle pour vérifier que leur prix de transfert est économiquement justifié.

Enfin, la question se pose de savoir s'il est souhaitable de taxer ces transferts. Le seul avantage qui semble en découler serait des ressources supplémentaires pour le gouvernement. Il est en effet à craindre que cette taxation
non seulement freine le développement de l'industrie des services d'information dans le pays et nuise à sa compétitivité au niveau international, mais de plus les autres pays risquent de prendre des mesures de rétorsion et d'étouffer plus encore cette industrie (56).

De plus, l'extension du contrôle des gouvernements sur les informations pourrait être considérée comme une forme de censure, attentatoire aux libertés publiques.

Paragraphe 3 : La détermination de la loi applicable

A la jonction des intérêts privés et publics se trouve la question de la loi applicable. En effet, la détermination de cette loi intéresse autant les parties privées, qui veulent savoir quelle réglementation s'appliquera à leur convention et quelles dispositions elles doivent respecter, que les Etats, soucieux d'éviter les applications extra-territoriales des lois et les empiètements sur leur souveraineté.

Pour les contrats internationaux, c'est-à-dire mettant en cause les intérêts économiques d'au moins deux pays, ce qui est bien notre hypothèse pour les services télématiques internationaux, le principe accepté par la majorité des pays est celui de l'autonomie de la volonté, selon lequel les parties choisissent et indiquent dans leur convention la loi nationale qui régira leurs relations.

Dans la mesure où une convention tient lieu de loi à ceux qui l'ont faite (art. 1134 C. civ.), la loi choisie par les parties a vocation à s'appliquer à titre supplétif, c'est-à-dire lorsque le contrat ne fournit pas de solution au litige.

Lorsque les parties n'ont pas indiqué la loi applicable, le juge compétent détermine leur volonté sur ce point à l'aide des éléments du contrat. Pour ce faire, il cherche le "centre de gravité" de l'opération, c'est-à-dire l'ordre juridique national avec lequel elle a le plus de contacts en prenant en considération le lieu de conclusion du contrat, le lieu d'exécution de la prestation caractéristique ou d'autres éléments spécifiques au contrat en cause. On appelle cette opération la localisation du contrat.

Enfin, le juge a la possibilité de remettre en cause le choix des parties lorsque la loi indiquée dans le contrat n'a aucun lien avec l'objet de la convention, afin d'éviter les fraudes (choix par les parties d'une loi qui autorise par exemple une transaction que leur loi interdit ou soumet à des conditions plus sévères) et utilise à cette fin la technique de la localisation.

En matière de services télématiques internationaux, il n'existe que peu de réflexions sur la question de la loi applicable, généralement centrées sur les réglementations nationales restrictives, le besoin ou non d'une convention internationale et les recherches des organisations internationales sur ce point (57).

En effet, les aspects de droit international privé des F.T.D. ont d'abord été perçus en matière de protection de la vie privée. Les experts de l'O.C.D.E., lors de l'élaboration des lignes directrices sur les flux transfrontières de données personnelles, se sont inquiétés de la législation applicable à ces flux. A cette occasion, ils ont reconnu que la technique traditionnelle de localisation apparaît comme peu adaptée aux F.T.D. en raison de la rapidité du mouvement des données, de la dispersion géographique que peut connaître une même opération et de la multiplicité des intervenants. Cette situation multiplie le nombre de facteurs de rattachement et complique en conséquence le choix de l'un d'eux, d'autant plus qu'il n'est pas sûr que les techniques traditionnelles derattachement soient applicables auxnouvellestechnologies (58).
Ainsi, les critères utilisés habituellement pour déterminer le pays avec lequel la transaction a le plus de contacts n'ont plus la certitude et la fixité requises. Le lieu de conclusion peut être fortuit, voire même inexistant pour les contrats passés par voie télématique (situation cependant

hypothétique pour les services télématiques professionnels); le lieu d'exécution est-il celui où est situé l'ordinateur ou l'utilisateur ? ; faut-il retenir la loi du lieu du dommage ou du fait dommageable?

Ce dilemne est illustré par la proposition faite en juin 1980 au sein de l'O.C.D.E. par la délégation des Etats-Unis sur les solutions qui pourraient être retenues. Selon cette proposition, on pourrait choisir entre (59)

> "... la loi de l'Etat dont la personne concernée est ressortissante, la loi de l'Etat dont le maître de fichier est ressortissant, la loi de l'Etat où s'effectue le traitement primaire et le stockage des données, la loi de l'Etat où les décisions sont prises en fonction des données, la loi de l'Etat dont l'utilisateur effectif est ressortissant ou bien recourir à un droit international positif ou procédural entièrement nouveau élaboré spécialement."

En matière de données nominatives, une solution possible consiste à retenir la loi nationale qui offre la meilleure protection à ces données. De même en cas de dommage, la loi allemande prévoit l'application de la loi la plus favorable à la victime. Cette solution laisse cependant subsister trop d'incertitudes quant à la loi qui sera finalement appliquée. Le fournisseur du service télématique ne sait à quelle réglementation se conformer pour exercer son activité dans la légalité et les clients qui ont subi un dommage ne connaissent pas leurs droits et les moyens d'action qui leur sont ouverts.

La question de la loi applicable aux F.T.D. n'est pas simple, et il est significatif de constater que les lignes directrices de l'O.C.D.E. se contentent d'inviter les pays membres à établir des principes qui permettront de déterminer cette loi (article 22 des lignes directrices et commentaires n° 74-75 et 76). Mais il est clair que cette question se pose pour tous les types de flux, et notamment les flux de données commerciales dont le volume augmente et qui soulèveront probablement un plus grand nombre de litiges que les flux de données nominatives.

Pour arriver à une harmonisation internationale de la loi applicable aux F.T.D., trois solutions peuvent être envisagées (60).

La première consiste à élaborer des clauses-type indiquant de façon explicite le droit applicable au contrat et parmi lesquelles les parties pourraient choisir. Ces clauses seront

respectées dans la plupart des pays, mais du fait qu'elles seront nécessairement interprétées par référence à la loi du lieu du jugement (lex fori), il pourra tout de même en résulter des divergences d'interprétation, en particulier lorsque le choix d'une loi étrangère permet de contourner l'application d'une disposition légale impérative. De plus, le choix explicite d'une loi applicable ne résoud pas le problème de savoir si une obligation contractuelle a été créée ou non, et donc si elle a été respectée.

L'élaboration de clauses-types résoudrait un certain nombre des problèmes juridiques de fond soulevés par les F.T.D. et encouragerait les parties aux services télématiques internationaux à jouer un rôle actif dans leur résolution.
Cependant elle est insuffisante pour mener à une harmonisation internationale complète du fait qu'en cas de silence des parties, les règles de conflit de loi restent variables selon les pays. Dans la plupart d'entre eux, le juge appliquera la loi qui a la relation la plus étroite et la plus importante avec la transaction, et en matière de services télématiques, il pourra considérer qu'il s'agit de la loi du pays dans lequel est implanté le fournisseur du service, mais les risques de solution contradictoire demeurent.

Une deuxième solution consisterait à prévoir dans un accord international des solutions explicites et des clauses-type. Cet accord pourrait même comprendre des règles de conflit et prévoir une procédure pour trancher les litiges portant sur les clauses-type. Cette solution, qui instaurerait une étroite coordination internationale, se heurte cependant à deux difficultés. La première est la nécessité d'intégrer les dispositions internationales dans le droit national des différents pays, ce qui implique la mise en oeuvre de procédures lourdes et souvent longues (par exemple les lois de ratification de certains pays). Ensuite cet accord ne supprime pas les risques de divergence puisque ces dispositions seront interprétées par les juridictions nationales, donc susceptibles d'interprétations variables et de jugements contradictoires pour un même litige.
Enfin l'élaboration d'une convention internationale est un projet de longue durée et en cela même peu recommandé dans un domaine où les technologies évoluent rapidement et où les politiques nationales ne sont pas encore claires.

La meilleure solution semble donc être une Recommandation Internationale prévoyant des clauses-type et des règles de conflit, et dont la mise en oeuvre serait à la fois souple et informelle tout en assurant une certaine sécurité par l'harmonisation des règles de conflit. Une organisation internationale pourrait d'ailleurs être chargée d'observer la pratique dans ce domaine et de modifier les clauses-type en cas de nécessité.

A quelle organisation confier cette tâche? La proposition de la délégation des Etats-Unis mentionnée plus haut laisse penser que l'O.C.D.E. ne serait pas l'instance la plus compétente pour assumer cette fonction, et suggère de l'attribuer à la Conférence de La Haye de Droit International Privé, spécialisée depuis longtemps dans les problèmes de conflit de lois et qui regroupe à peu près les mêmes pays que l'O.C.D.E. Pour sa part, M. BING, propose de créer une nouvelle organisation internationale à cet effet mais il est à craindre que cette solution soit trop lourde à mettre en oeuvre et c'est pourquoi la Conférence de la Haye apparait comme un meilleur choix (61).

Dans l'hypothèse qui nous occupe, à savoir les services télématiques professionnels, la solution à la question de la loi applicable pourrait être trouvée dans les textes internationaux relatifs à la vente internationale de biens. Nous avons relevé deux de ces textes.

La Convention de La Haye portant sur la loi applicable à la vente internationale d'objets mobiliers corporels a été adoptée à la 7ème session de la Conférence de La Haye en 1951 et est internationalement entrée en vigueur le 1er septembre 1964 (62).
Bien que ses dispositions concernent la vente de biens corporels, on peut imaginer leur extension et leur adaptation aux services télématiques internationaux (63).

L'article 2 al. 1 de cette convention consacre la loi d'autonomie :

> "La vente est régie par la loi interne du pays désigné par les parties contractantes".

Cette formulation permet de résoudre deux des difficultés qui surgissent souvent en matière de conflit de loi : en précisant qu'il s'agit de la loi interne, la Convention exclue à la fois le jeu du renvoi et le rattachement au droit international ou à la très controversée "lex mercatoria".

Lorsqueles parties ont gardé le silence ou n'ont pas exprimé clairement leur volonté, la loi applicable est, selon l'article 3 de la Convention, "...la loi interne du pays où le vendeur a sa résidence habituelle au moment où il reçoit la commande".

Dans notre espèce, il s'agirait du lieu d'établissement du fournisseur du service télématique.

Cette solution trouve une confirmation dans la Convention européenne sur la loi applicable aux obligations contractuelles ouverte à la signature à Rome le 19 juin 1980 (64).

Du fait qu'elle s'applique aux obligations contractuelles en général, cete Convention ne rencontre pas l'objection faite à la précédente par le caractère incorporel des services télématiques.

Elle réaffirme le principe d'autonomie (article 3) et, à défaut de choix par les parties, dispose que le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits (article 4, alinéa 1). Cette loi est présumée être celle du pays où la partie qui doit fournir la prestation caractéristique a, au moment de la conclusion du contrat, sa résidence habituelle ou s'il s'agit d'une personne morale son administration centrale (article 4, alinéa 2).

Cette disposition désigne de nouveau le fournisseur du service télématique. La suite de l'article précise que si le contrat est conclu dans l'exercice de l'activité professionnelle, ce qui est notre cas, la loi applicable est celle du pays où est situé son principal établissement ou si le contrat le précise et qu'il est différent, l'établissement qui fournit la prestation.

En conclusion lorsque les parties à un contrat de service télématique n'ont pas clairement exprimé leur choix quant à la loi applicable, on peut estimer que celle-ci est présumée être la loi du pays où est établi le fournisseur du service. Cette solution est renforcée non seulement par la reconnaissance du principe dans deux conventions internationales, mais également par son adéquation à la pratique.

CONCLUSION

Les services télématiques se situent par nature dans un contexte international, et participent à l'internationalisation de l'économie. Sur le plan juridique, cette internationalisation va et doit entraîner une modification des mentalités, et notamment l'habitude de penser au niveau national car cette attitude non seulement constitue souvent un frein au progrès, mais elle risque surtout de vider le droit de toute signification du fait qu'il n'a plus aucun rapport avec la réalité.

On doit cependant constater que si des principes dans ce sens existent en droit international, on peut leur reprocher d'être trop vagues, peu pratiques et en conséquence peu appliqués. Une preuve en est que ce sont les principes les plus pragmatiques, et en particulier la normalisation, qui ont eu jusqu'à présent le plus d'effet.

Une pensée juridique pratique et internationale permettrait d'aboutir à une conciliation entre les pays, à une collaboration qui, au lieu de freiner les transferts de données les favoriserait en leur apportant sécurité et légitimité et constituerait une appréhension positive par le droit de la télématique.

En effet, on peut estimer que le droit s'est montré jusqu'à présent très négatif vis-à-vis des nouvelles technologies, ce qui risque de le reléguer à l'arrière-plan au lieu de lui laisser jouer son rôle de modérateur et protecteur.

Ainsi, les attitudes restrictives de certains pays sont tout à fait compréhensibles, et ne sont motivées que par l'absence d'un droit international qui les protège efficacement. Et il apparaît que cette absence est due en partie à l'idée, soigneusement entretenue par certains, qu'une libre circulation des données est nécessairement contradictoire à leur protection, alors que ces deux principes sont complémentaires et que le droit international peut les concilier.

NOTES

(1) International Institute of Communication (I.I.C.), "Transborder flows of personal and non-personal data", London (1983), p.1.
Jane A. ZIMMERMAN, "Transborder Data Flows : Problems with the Council of Europe Convention or Protecting States from Protectionism", Northwestern Journal of International Law and Business, 4 : 61 (1982), p. 620.

(2) "Transborder Data Flows : Proceedings of an O.E.C.D. Conference", North Holland, O.E.C.D., Amsterdam (1985), p. 41.

(3) Idem, p. 42.

(4) Commission Consultative Internationale pour le Développement des Flux Transfrontières de Données, "Etat de l'Art dans le Domaine des F.T.D.", I.B.I. Rome 1985, p. 1.

(5) Chambre de Commerce Internationale (C.C.I.), "Flux d'informations. Analyse des problèmes qui se posent aux entreprises", Doc. n. 373/23 Rev. 3, Paris (Décembre 1984), p. 3.

(6) K.W. GREWLICH, "Free Electronic Information and Data Flows", p. 55 et s.

(7) Ibid.,
I.I.C, précité n. 1, p. 2.
J. BING, P. FORSBERG and E. NYGAARD, "Problèmes juridiques posés par les flux transfrontières de données" in : "Une analyse préliminaire des problèmes juridiques dans l'informatique et les communications". PIIC n. 8, O.C.D.E. Paris (1983), p. 109.

(8) O.C.D.E., précité n. 2, p. 17.

(9) BING, précité n. 7, p. 296-97.

(10) Idem, p. 91-93.

(11) Idem, p. 92.

(12) Idem p. 94-95, O.C.D.E., précité n. 2, p. 20.

(13) BING, précité n. 7, p. 98-99.

(14) C. OLMSTEAD, "Transborder Data Flows; legal issues including conflict of laws", paper presented at the Conference on "Operational and Legal aspects of transborder data flows", organized in London on 16-17 October 1985 by the International Law Association p. 4.

(15) BING, précité n. 7, p. 100.

(16) Idem, p. 101.

(17) Idem, p. 103-104.

(18) Idem p. 102-108.

(19) J. DE HOUWER, "Privacy en grensoverschrijdend dataverkeer : een vergelijkende studie van internationale en nationale reglementeringen" in "Soft en hard, ware het niet om te fraude, bedenkingen over computercriminaliteit", I.U.S. n. 7, Kluwer rechstswetenschappen, Antwerpen (1985), p. 90.

(20) G.S. GROSSMAN, "Transborder Data Flows : Separating the Privacy Interests of Individuals and Corporations", Northwestern Journal of International Law and Business, Spring 82, volume 4, number 1, p. 3.

(21) J. DE HOUWER, précité n. 19; p. 91
"Guidelines governing the protection of privacy and transborder flows of personal data", 23 septembre 1980, Explanatory Memorandum, Paragraphes 50 à 62.

(22) DE HOUWER, précité n. 19, p. 92-93.
I.I.C., précité n. 1, p. 8-9.

(23) DE HOUWER, précité n. 19, p. 94.

(24) I.I.C., précité n. 1, p. 10.

(25) Résoluion 73 (22) sur la protection de la vie privée des individus vis-à-vis des banques de données électroniques dans le secteur privé;
Résolution 74 (29) sur la protection de la vie privée des individus vis-à-vis des banques de données électroniques dans le secteur public.

(26) ZIMMERMAN, précité n. 1, p. 620.

(27) Idem, p. 622.

(28) Idem, p. 623.

(29) DE HOUWER, précité n. 19, p. 98-99.
Mémorandum précité n. 20, paragraphes 63-68.

(30) Mémorandum, paragraphe 66.

(31) DE HOUWER, précité n. 19, p. 99.

(32) Idem, p. 110-115.
J. DE HOUWER, "Privacy and Transborder Data Flows", Computer and Law, V.U.B. Centrum voor Internationaal Strafrecht, Bruxelles (Novembre 1984).

(33) C. COLOMBET, "Propriété littéraire et artistique", Précis Dalloz, Paris (1976), p. 319-326.

(34) Idem, p. 328.

(35) BING, précité n. 7, p. 105.

(36) M. POULLET, "La Télématique", Les Nouvelles Editions Marabout, Alleur (1985), p. 78-79.

(37) BING, précité n. 7, p. 106.

(38) Directives du Conseil de la Communauté du 28 mars 1983, J.O.C.E. 26/4/1983, n. L 109/8.

(39) BING, précité n. 7, p. 108.

(40) United Nations Centre on Transnational Corporations, "Transnational Corporations and transborder Data Flows : a technical paper", United Nations, ST/CTC/23, New York (1982), en particulier p. 48 et s.

(41) ZIMMERMAN, précité n. 1, p. 617-619.

(42) M.D. KIRBY, "Aspects juridiques de la technologie de l'information", in P.I.I.C. n. 8, précité n. 7 p. 41 I.I.C., précité n. 1, p. 20;
M. MASMOUDI, "The New World Information Order", U.N.E.S.C.O., SC/MD/63 (1979).

(43) "Telecommunications and Canada", Ottawa, Canadian Government Publishing Centre (1979).

(44) "Transborder Data Flows said to be impeded by trade restrictions in foreign countries", International Trade Reporter, 26/02/86, vol. 3, p. 280-281.

(45) MARK B. FELDMAN et DAVID R. GARCIA,"National Regulation of Transborder Data Flows", North Carolina Journal of International Law and Commercial Regulation, vol. 7, Winter 1982, Number 1, p. 1-25.

(46) United Nations, précité n. 40, p. 75.

(47) Commission of the European Community, "European Society faced with the challenge of New Information Technologies : A Community Response", Bruxelles (1979).

(48) FELDMAN et GARCIA, précité n. 45, p. 11.

(49) United Nations, précité n. 40, p. 73.
United Nations Centre on Transnational Corporations, "Transborder Data Flows and Brazil", United Nations, ST/CTC/40, New York (1983).

(50) FELDMAN et GARCIA, précité n. 45, p. 13.

(51) Idem, p. 21.

(52) Idem, p. 22.

(53) Idem.

(54) O.C.D.E., précité n. 2, p. 20.

(55) Idem.

(56) Idem.

(57) OLMSTEAD, précité n. 14, p. 5.

(58) KIRBY, précité n. 42, p. 38.

(59) Idem, p. 40.

(60) BING, précité n. 7, p. 124 et s.

(61) Idem, p. 126.

(62) Y. LOUSSOUARN et J.D. BREDIN, "Droit du Commerce International", Sirey, Paris (1969) n. 503 et s., en particulier n. 570 et s.

(63) KIRBY, précité n. 42, p. 40.

(64) Convention 80/934/C.E.E., J.O.C.E. du 9/10/80, n. L 266/1 à 7.