Les nouvelles technologies : un défi pour la protection de la vie privée ? (1989)

Etude préparée par le Comité d'experts sur la protection des données (CJ-PD) sous l'égide du Comité européen de coopération juridique (CDCJ), Strasbourg 1989

TABLE DES MATIERES

1. Introduction

1.1. Historique

Lors de l'élaboration des normes sur la protection des données, au cours des années 70, le législateur, tant au niveau national qu'international, a pris comme point de départ l'état de la technologie informatique existant et a apporté des solutions juridiques aux problèmes qui étaient alors perçus et que l'utilisation des nouvelles technologies posait aux individus Il s'agissait d'insérer cette technologie dans un cadre juridique afin de réduire au minimum les dangers de l'ordinateur et de permettre en même temps à l'informatique de se développer librement pour apporter ses bénéfices reconnus à la société.

Les solutions envisagées en 1970 étaient valables dans la mesure où elles étaient sensées s'appliquer à la situation d'alors, caractérisée par de gros ordinateurs autonomes ayant des applications spécifiques, et capables d'enregistrer et de traiter des données relatives à «des personnes identifiées ou identifiables», sur un «fichier» sous l'autorité d'un «maître du fichier» qu'une autorité de contrôle pouvait identifier à souhait.

Toutefois, la technologie n'est pas restée figée; elle a rapidement dépassé les normes existantes et appelle de nouvelles réponses de la part du législateur. Alors que ce

dernier mettait la touche finale aux textes législatifs reflétant l'état de la technologie des années 70, des progrès rapides sont intervenus dans le domaine informatique, caractérisés par une explosion du nombre des ordinateurs, un développement de leurs capacités, une réduction de leur coût et par leur pénétration croissante dans les foyers, les entreprises et les administrations. Les conséquences de l'apparition de systèmes informatiques décentralisés et répartis, ayant d'énormes capacités de collecte, d'enregistrement et de traitement de données à caractère personnel, capables de dialoguer avec un terminal sur de longues distances, ont forcé le législateur à s'interroger sur la pertinence de l'approche adoptée. Tout cela a été rendu possible par le rapide développement des télécommunications dont les ingénieurs ont été capables d'exploiter l'ingéniosité des informaticiens afin de rendre compatibles deux technologies auparavant distinctes. Le mariage de l'informatique et des télécommunications a non seulement permis une plus grande diffusion des systèmes informatiques et une plus grande dissémination des données qui allaient mettre en question les concepts existants mais a également produit toute une gamme de services télématiques qui ont peu à peu commencé à poser leurs propres problèmes.

1.2. Mandat

Le Conseil de l'Europe, qui s'est efforcé de montrer la voie aux législateurs nationaux en matière de protection des données en préparant et ouvrant à la signature la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («Convention pour la protection des données») du 28 janvier 1981, a lui-même commencé à réfléchir sur l'impact des technologies de l'information sur les normes de la Convention, insérées dans les législations des Parties contractantes ou reprises par les Etats en train d'élaborer des règles dans ce domaine. C'est pour cette raison que le Comité d'experts sur la protection des données (CJ-PD) a demandé expressément l'autorisation du Comité des Ministres du Conseil de l'Europe pour inclure, dans son futur mandat, une analyse de l'impact de certaines des nouvelles technologies pour la protection des données:

«Examiner attentivement l'impact des technologies suivantes pour la protection des données et préparer tout instrument juridique nécessaire:

i. la télémétrie;

ii. les médias interactifs;

iii. les systèmes de courrier électroniques»

En procédant à cet examen, le comité d'experts s'était déjà accoutumé au type de problèmes créés par l'introduction et l'utilisation des nouvelles technologies. Outre les informations recueillies par le biais des échanges de vues parmi les experts au cours des différentes réunions, le comité a tiré grand profit des rapports scientifiques présentés au 14'Colloque de droit européen qui s'est tenu à Lisbonne du 24 au 26septembre 1984 sur le thème: «Au-delà de 1984: le droit et les technologies de l'information dans la société de demain.» La réflexion du comité a été en outre alimentée par les exposés présentés par les deux experts consultants en matière de nouvelles technologies lors de la 11e réunion (16-19 avril 1985), les professeurs Arnbak (Pays-Bas) et Chamoux (France).

1.3. Approche adoptée par le groupe de travail

Le groupe de travail chargé d'examiner la question a tenu sa première réunion du 16 au 18 décembre 1985. Cette réunion lui a permis d'avoir une vue d'ensemble des problèmes que les trois types de technologie posent pour les systèmes de protection des données. Afin d'approfondir son travail, le groupe décida de demander aux Etats membres des informations supplémentaires sur leurs expériences en ce qui concerne l'introduction et l'utilisation de la télémétrie, des médias interactifs et du courrier électronique, notamment du point de vue des problèmes qui se posent et des réponses juridiques qui sont apportées par les Etats membres à de tels problèmes. Les réponses fournies par les Etats membres se sont basées sur les définitions de travail suivantes des nouvelles technologies en question, définitions élaborées lors de la première réunion du groupe de travail:

i. Télémétrie

La collecte à distance, par le biais de procédés automatiques, de données à caractère personnel sans que la personne concernées joue de rôle actif dans le processus de collecte de ces données.

ii Médias interactifs

Systèmes télématiques offrant la possibilité d'un dialogue instantané entre un individu et de tels systèmes, en vue d'obtenir et de transmettre des informations, à l'initiative de cet individu.

iii. Courrier électronique

Systèmes télématiques d'enregistrement et de transmission de communications interpersonnelles permettant, suivant le cas, d'envoyer des messages ou d'accéder à de tels messages par le biais d'un dispositif central; l'envoi de ces messages étant sous le contrôle de l'expéditeur et la réception sous le contrôle du destinataire.

Il est important de souligner que le groupe de travail, au cours de ses réunions ultérieures consacrées à la rédaction de ce rapport (1-3 octobre 1986; 16-18 mars 1987), n'a pas considéré les définitions ci-dessus ni les concepts eux-mêmes comme parfaits ou définitifs. Les réponses au questionnaire confirment les difficultés que l'on peut rencontrer en essayant de classer dans des catégories préétablies de nouveaux phénomènes technologiques. Le danger existe d'exclure certains dispositifs techniques que l'on ne peut pas classer immédiatement dans la catégorie de la télémétrie, des médias interactifs ou du courrier électronique. Par exemple, dans quelle catégorie faut-il classer les systèmes experts et la téléconférence? Pour cette raison, il a été jugé souhaitable, d'une part, de garder à l'esprit, dans la suite des travaux, le fait que les termes mentionnés dans le mandat pourraient avoir une application plus étroite ou plus large et, d'autre part, d'illustrer chacune des définitions d'exemples basées sur les réponses au questionnaire En outre, rechercher à tout prix une définition précise pourrait éventuellement avoir pour conséquence d'occulter les problèmes créés par le contexte plus large qui a donné naissance à ces technologies, à savoir la nouvelle infrastructure technologique créée par les télécommunications et le traitement des données, C'est ce dernier aspect, et notamment les possibilités offertes par le caractère

multifonctionnel des réseaux de télécommunications et le développement des flux de données, qui constitue le point commun de référence non seulement pour la télémétrie, le courrier électronique et les médias interactifs mais également pour toutes les autres technologies. L'analyse des tendances technologiques, présentée au chapitre 2, est donc utile non seulement pour replacer dans son contexte la discussion sur les trois technologies spécifiques mais également pour permettre en fin de compte d'identifier les problèmes et enjeux plus larges qui touchent aux concepts actuels de la protection des données face à la technologie en général,

1.4. Structure du rapport

Gardant à l'esprit la nature de l'analyse contenue dans le chapitre 2, chacun des termes utilisés dans le mandat fait l'objet d'une analyse descriptive, le point de départ étant les définitions de travail générales utilisées pour les besoins du questionnaire; les informations reçues sont par contre analysées du point de vue des services/caractéristiques techniques et du point de vue des normes existantes ou envisagées dans les Etats membres pour chacune des technologies. A partir d'une identification des problèmes de protection des données posés par chacune de ces technologies, le rapport tente d'attirer l'attention des Etats membres sur les différentes façons de les aborder.

Il n'est pas envisagé de trouver des solutions juridiques pour les différents problèmes identifiés dans le rapport. Les Etats membres pourront, espérons-le, tirer profit des approches adoptées dans certains pays. En d'autres termes, les diverses options possibles pour résoudre les problèmes posés par les différentes technologies sont mises en évidence afin de laisser aux Etats la possibilité de développer leur propre politique conformément à ce qu'ils pensent être la meilleure approche dans ce domaine.

Au-delà des problèmes particuliers qui se posent, il est jugé important de placer la discussion à un niveau plus général en analysant les défis que ces trois technologies représentent pour les concepts existants de la protection des données. Pour cette raison, le chapitre 6 invite les gouvernements à s'interroger sur l'actuelle flexibilité des normes existant dans le domaine de la protection des données, face à ce nouvel environnement technologique.

2. Tendances actuelles des technologies

Comme il a été souligné lors du 14' Colloque de droit européen, les nouvelles technologies sont en état de réunir toutes les techniques déjà connues (informatique, téléphone, télex, télévision, etc.) et de les améliorer considérablement du point de vue qualitatif et quantitatif.

Le mariage de l'informatique et des télécommunications, baptisé en France du nom de «télématique», a ainsi ouvert d'énormes perspectives dans tous les pays. Il a bouleversé les moyens traditionnels de diffusion de l'information (imprimerie, édition, etc.) ainsi que le secteur des services. Comme le notait le professeur Arnbak lors de son rapport devant le Comité d'experts sur la protection des données (CJ-PD), le marché mondial du matériel de télécommunications et celui des services sont aujourd'hui beaucoup plus importants que celui des ordinateurs. On peut citer à ce

propos l'exemple de la France où les seuls services c<kiosque» du Minitel ont rapporté aux serveurs et aux éditeurs 360 millions de francs français de recettes au cours des six premiers mois de 1986, au lieu de 260 millions de francs français sur les douze mois de 1985. On mesure donc tout l'enjeu économique et industriel de ces nouvelles technologies pour nos sociétés.

L'information, élément essentiel de notre vie, est devenue valeur marchande et il est désormais intéressant de la «capitaliser», d'où la multiplication spectaculaire des banques de données ces dernières années: banques de données à usage général, souvent internationales, et multitude de banques dites «locales», mises en place par la presse, les collectivités locales ou les administrations.

Mais l'information en elle-même n'a de valeur que si elle est accessible rapidement et à distance par l'intermédiaire de réseaux. Les investissements nécessaires à la mise en place des infrastructures appropriées sont considérables et expliquent d'autre part le besoin de rechercher l'utilisation la plus rentable des matériels informatiques. Ce souci de rentabilité conduit à l'interconnexion de ces réseaux, de manière à répartir leurs charges et leurs bénéfices, et à l'intégration de plusieurs services dans un même réseau. Déjà se profile à l'horizon la mise en place d'un réseau unique multifonctionnel, intégrant les réseaux traditionnellement distincts du téléphone, du télex et du traitement des données: il s'agit de L'ISDN (integrated Services Digital Network) ou Réseau numérique intégré de services (RNIS). Cela est techniquement possible grâce à la numérisation des réseaux et des services: lorsque le téléphone, le télex ainsi que les images fixes et mobiles sont représentés sous forme d'octets, il est possible de les traiter par un système numérique commun et dans un réseau commun. En outre, les réseaux distincts de télédistribution peuvent également être intégrés à ce réseau numérique pour former ce qu'on appelle l'IBC (integrated Broadband Communications) ou communications intégrées à bandes larges.

Dans le contexte de la communication par câble, il convient de mentionner également les fibres optiques qui augmentent considérablement les capacités de transmission et ouvrent des possibilités nouvelles dans le domaine des liaisons interactives c'est-à-dire bilatérales.

Les satellites de communication sont un autre exemple de réseaux multifonctionnels qui, servant tout d'abord à transmettre des conversations téléphoniques, sont maintenant employés de plus en plus pour échanger des émissions de télévision entre organismes de diffusion.

Cette évolution technique vers un accroissement des réseaux multifonctionnels et des interconnexions des systèmes de communications est renforcée par les mesures de normalisation, destinées à améliorer la compatibilité et la connectabilité des systèmes. En effet, seule une production de masse et donc des efforts dans le sens de la normalisation peuvent favoriser la rentabilité des systèmes de communication.

Les progrès techniques ont d'autre part permis un abaissement des prix des matériels informatiques, ce qui favorise leur diffusion auprès du grand public: le développement spectaculaire des micro-ordinateurs en quelques années en est le vivant exemple. Jusque-là réservées aux spécialistes, l'informatique, mais également les nouvelles technologies de l'information, sont à la portée d'un nombre croissant d'instances et

d'individus. Il semble d'autre part que, contrairement à d'autres techniques, l'informatique est plus facilement assimilée par la population et notamment par les jeunes. Parallèlement à ce phénomène, on assiste à une simplification de l'usage du matériel informatique On peut citer à ce titre les progrès effectués sur les logiciels de l'annuaire électronique (Minitel) en France, qui permettent de rechercher des noms propres sans en connaître l'orthographe exacte, où des noms de localités sans connaître leur situation géographique. Principalement orienté vers l'annuaire électronique au stade de la conception, le Minitel a aujourd'hui de nombreuses autres applications,

Les conséquences de l'évolution technique que l'on vient de décrire sont de deux ordres.

Premièrement, la pénétration de l'informatique dans la société fait que celle-ci devient «domestique». On peut d'ores et déjà imaginer le développement de la bureautique au niveau des foyers, ce qui permettra de gérer la correspondance et les affaires privées dans les mêmes conditions qu'une entreprise. Plus loin, la télédistribution interactive offrira, grâce à un clavier et un simple écran de télévision, de multiples possibilités: surveillance des malades à domicile, surveillance des maisons d'habitation contre les voleurs, sondages d'opinion immédiats, télémesure des compteurs par les entreprises concernées, enregistrement de programmes de télévision, consultation de banques de données, délivrance de programmes vidéo, enregistrement de programmes de télévision, programmation du four, de la machine à laver, etc.

On assistera donc, peu à peu, à une banalisation du phénomène informatique, ce qui constitue en soi un danger, les personnes concernées n'étant pas vraiment conscientes de toutes les conséquences de ces actes «technologiques». On a en effet désormais la possibilité de surveiller totalement un individu.

D'autre part, l'information est aujourd'hui en mesure de circuler, de se disséminer et de se disperser dans des conditions telles qu'il devient de plus en plus difficile de la protéger.

La deuxième conséquence de l'évolution technique décrite plus haut est qu'il devient pratiquement impossible d'isoler l'utilisation de l'informatique des autres activités, ce qui rend le travail des juristes d'autant plus compliqué. En effet, quelles règles juridiques faut-il appliquer à un réseau particulier sachant qu'il peut à la fois intégrer des informations pouvant circuler librement (programmes de télévision) et des informations à caractère personnel dont l'accès devrait être réservé à certaines personnes? Comme le notait le professeur Arnbak, le cadre juridique dépend moins aujourd'hui de la technologie appliquée et les réglementations classiques, qui sont basées sur une technologie particulière (droit de la pressé, de la télévision, etc.), risquent d'être rapidement dépassées. Les tendances vers des réseaux publics intégrés et des interconnexions de systèmes, accélérées par le progrès économique et une meilleure exploitation des systèmes, risquent de mettre en conflit des principes juridiques fondamentaux, si ces derniers devaient se baser sur des critères ou des notions trop technologiques.

Le professeur Arnbak propose en conséquence de définir des catégories de services de télécommunication auxquelles on pourrait appliquer les mêmes règles juridiques. Il

s'agit de distinguer les divers types de circulation de l'information entre les partenaires de la communication et d'analyser les pouvoirs relatifs et les positions relatives des participants à ce processus en répondant aux questions suivantes:

1. Qui contrôle le transfert de l'information (pour ce qui est du choix du moment, du sujet, de la fréquence, etc.): une institution ou les participants individuels?

2. L'information provient-elle d'une institution ou d'une personne privée?

Les réponses combinées à ces deux questions permettent de dresser le tableau suivant qui montre quatre modèles de circulation de l'information (modèles qui ont été établis par le professeur en télécommunication J.L. Bordewijk et par le journaliste B. van Kaam).

	Information provenant d'une source individuelle	Information provenant d'une source centrale
Choix individuel du moment, - du sujet, etc.	Conversation	Consultation
Choix central du moment, du sujet, etc.	Enregistrement	Allocution

Le professeur Arnbak tire les conclusions suivantes de l'analyse de ce tableau:

- les problèmes de droits d'auteur apparaissent dans la colonne de droite;

- les problèmes de protection de la vie privée interviennent dans la colonne de gauche;

- les procédures de contrôle et l'intervention de l'Etat paraissent souhaitables dans la rangée inférieure;

- par contre, dans les services de la rangée supérieure, il convient d'assurer la libre circulation de l'information et de réduire l'intervention de l'Etat au minimum.

Les rédacteurs de ce rapport ont estimé que cette analyse était particulièrement intéressante dans sa manière de cerner et d'identifier les différents problèmes posés par la télémétrie, les médias interactifs et les systèmes de courrier électronique. Cela leur a permis, qui plus est, d'élargir les discussions de manière à prendre en compte toutes les technologies en général. C'est pour cette raison qu'il est fréquemment fait référence dans ce rapport aux modèles de circulation de l'information mentionnés ci-dessus.

3. Télémétrie

3.1. Description des services et caractéristiques techniques

Si l'on se réfère aux modèles de circulation de l'information décrits précédemment, la télémétrie entre dans la catégorie de l'enregistrement de données: collecte ou

classement par un organe central d'informations provenant d'individus, à des moments choisis au point central. On peut citer comme exemples: les systèmes de surveillance électronique (détecteurs de son, caméras vidéo, etc.), relevés à distance des compteurs de consommation pour l'eau, l'électricité ou le gaz, identification des plaques d'immatriculation des véhicules, mesure du nombre d'erreurs commises par une dactylo, connaissance des émissions de télévision regardées par un individu, surveillance des personnes âgées à domicile, etc.

Deux éléments se dégagent de cette dernière définition: l'enregistrement de données à distance et la non-intervention de la personne concernée, qui ne sait pas quand il y a enregistrement de données ou qui peut même ignorer que des données sont enregistrées à son sujet.

Le contenu même de la définition établie par le groupe de travail (voir paragraphe 1.3 ci-dessus) n'a pas posé grand problème, la plupart des experts s'accordant sur les services correspondant au terme télémétrie. Il a toutefois été signalé que la saisie sur un terminal d'ordinateur de données comportant des informations nominatives pourrait entrer dans le champ d'application de cette définition. Il a par conséquent été proposé de préciser, dans la définition de travail, que le traitement est entièrement automatisé. Pour ce qui est du terme télémétrie lui-même, il a été suggéré d'utiliser en français le mot «télémesure», qui paraît plus approprié.

3.2. Situation dans les Etats membres et réglementations existantes ou envisagées

Bien que la télémétrie puisse paraître un phénomène nouveau, la mesure à distance existe en fait depuis un certain temps notamment en ce qui concerne l'enregistrement des communications d'un abonné au téléphone. Il semble, toutefois, qu'en dehors du téléphone, il y ait très peu d'applications de cette technique dans les Etats membres du Conseil de l'Europe. Les exemples suivants peuvent être cités:

Belgique: télémaintenance des centraux téléphoniques qui peuvent être programmés à partir de la société installatrice;

République Fédérale d'Allemagne: lecture de compteurs à distance pour l'électricité (système Temex). Un système analogue est envisagé pour la consommation d'eau;

France: installation d'autocommutateurs dans les entreprises (système d'enregistrement des numéros d'appel);

Espagne: système de transmission et de réception d'électrocardiogrammes à partir de navires;

Pays-Bas: plusieurs municipalités envisagent l'utilisation des réseaux locaux de télévision par câble pour relever la consommation du gaz, de l'électricité et de l'eau dans les foyers;

Norvège: un système analogue est envisagé pour le relevé de la consommation d'électricité.

On constate donc que la République Fédérale d'Allemagne est pratiquement le seul pays où un système de télémétrie est appliqué à grande échelle: le service Temex. Ce dernier fait l'objet de dispositions spéciales dans le code des télécommunications. Aux termes de l'article 8, les fournisseurs du service Temex doivent informer leurs clients des circonstances, de l'ampleur, de la date et de l'heure de la transmission des informations. L'article 9 stipule que les informations télémétriques qui contiennent des données à caractère personnel peuvent être enregistrées temporairement par la Deutsche Bundespost, exclusivement à la demande d'une entreprise de service public et uniquement afin de déterminer l'importance de la consommation de ses clients. Cette information visant à déterminer la consommation n'est enregistrée que dans la mesure nécessaire à l'établissement des tarifs pour les biens consommés; cette information est transmise au fournisseur de services dans un délai de quatre jours; après quoi elle doit être effacée dans les services de la Deutsche Bundespost.

La loi sur la protection des données du Land de Hesse contient également un article relatif à la télémétrie et à la télésurveillance. Celui-ci stipule que toute personne utilisant un système télémétrique ou tout autre système de surveillance à distance, placé dans la résidence d'un individu ou sur son lieu de travail, doit obtenir le consentement préalable de cet individu.

En Belgique, la télémaintenance des centraux téléphoniques est régie par le droit contractuel.

En France, l'introduction et l'utilisation des systèmes télémétriques sont couvertes par la loi du 6 janvier 1978 sur l'informatique et les libertés. Cette loi institue un système de déclaration simple en ce qui concerne le secteur privé et un système d'avis avec publication d'un acte réglementaire en ce qui concerne le secteur public. L'article 29 précise que toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles soient déformées ou communiquées à des tiers non autorisés.

En Norvège, les registres constitués pour les besoins de la télémétrie sont couverts par la loi sur la protection des données et le Service d'inspection des données est habilité à réglementer la manière dont les informations peuvent être recueillies. Il peut aussi interdire l'utilisation de la télémétrie ou suggérer d'autres solutions.

3.3. Analyse des problèmes de protection des données

Les services offerts par la télémétrie étant divers, il est certain que les problèmes posés en matière de protection des données ne sont pas les mêmes. Ainsi, la surveillance à distance d'une maison ne pose pas tellement de problèmes de protection des données, contrairement au relevé automatique d'un compteur ou à l'enregistrement à distance des préférences des téléspectateurs pour telle ou telle émission.

L'une des premières caractéristiques de la télémétrie est que la personne concernée ne sait ni quand ni quelles données sont collectées à son sujet. L'enregistrement peut en effet avoir lieu à tout moment. Ainsi, le système télémétrique de consommation d'électricité envisagé en Norvège prévoit un relevé des compteurs des individus toutes les six minutes; auparavant, la lecture des compteurs était faite par une personne une

fois par an. On constate donc une grande différence entre le système antérieur et le système envisagé. Dans le deuxième cas, des informations très détaillées vont être recueillies, ce qui ne se justifie ni du point de vue de la consommation électrique des ménages, ni par des raisons de gestion ou de statistiques. Cette accumulation de détails représente un réel danger pour la vie privée notamment si ces informations sont utilisées à des fins détournées. Une crainte couramment évoquée est celle de «I'homme transparent», c'est-à-dire qui peut être surveillé constamment, totalement et à distance. Il découle de ces considérations que la personne concernée doit être informée que des données sont collectées à son sujet ainsi que de la fréquence de ces enregistrements. La question de la finalité du traitement est également essentielle dans ce contexte.

Un autre problème abordé est celui de la possibilité, pour le transporteur, d'enregistrer les informations collectées. On a vu, en effet, qu'en République Fédérale d'Allemagne, à la demande du prestataire de services, la Bundespost pouvait enregistrer les données collectées dans le cadre du service Temex. Ce cas semble toutefois assez unique mais il existe là un risque supplémentaire de détournement des informations, même si l'enregistrement est limité dans le temps.

On peut également s'interroger sur la nécessité de certains dispositifs, tels que ceux permettant de mesurer le nombre d'erreurs commises par une dactylo, qui ne semblent être utilisés que parce qu'ils sont techniquement possibles: il a été suggéré que, dans ces cas précis, il fallait trouver une limite à ce qui est acceptable.

Les droits d'accès et de rectification et le droit à l'oubli apparaissent également importants dans le contexte de la télémétrie.

Compte tenu des différents problèmes mentionnés ci-dessus, une éventuelle réglementation de ce secteur devrait tenir compte des éléments suivants:

1. Information préalable, voire, dans certains cas, consentement préalable, de l'individu devant faire l'objet d'une surveillance à distance ou soumis à un système télémétrique; si cela s'avère impossible, il convient de subordonner la collecte de données à une autorisation légale;

2. Information de la personne concernée sur la teneur de toutes les données recueillies, la fréquence et le moment de leur enregistrement ainsi que sur l'utilisation qui en sera faite;

3. Interdiction d'une utilisation secondaire des données et notamment la divulgation à des tiers;

4. Droit d'accès à ces données et, le cas échéant, droit de rectification;

5. Droit à l'oubli: les données enregistrées doivent être effacées après un certain laps de temps, compte tenu des délais de contestation.

4. Médias interactifs

4.1. Description des services et caractéristiques techniques

Le terme «médias interactifs» est suffisamment général pour permettre de couvrir une gamme d'applications technologiques. Lorsqu'un utilisateur disposant d'un terminal et de lignes téléphoniques peut obliger un ordinateur à répondre à des demandes émanant de lui, il est alors possible de parler d'interactivité. Ainsi décrits, les médias interactifs se différencient des systèmes télémétriques en ce que la personne concernée prend l'initiative de déclencher un processus automatisé qui conduit à une relation avec un tiers. Le modèle consultatif décrit au chapitre 9 constitue une description exacte de ce qui se passe dans les services électroniques d'informations, une des applications les plus communes des systèmes vidéotex. Le flux d'informations est déclenché par I'utilisateur qui veut consulter une base de données centrale afin d'obtenir des informations de la part d'un serveur. Le Télétex correspond également au modèle consultatif bien qu'il ne soit pas interactif à proprement parler puisqu'il ne permet pas l'envoi mais uniquement la réception d'informations.

Toutefois, il convient de souligner que les médias interactifs permettent également des transactions entre les utilisateurs et les serveurs, ce qui va au-delà d'une simple consultation de bases de données centrales. De plus en plus, les opérateurs de systèmes vidéotex permettent à leurs abonnés de se connecter à distance à des ordinateurs afin d'effectuer des transactions télébancaires ou de télé-achat; Dans ce cas, le modèle consultatif de circulation de l'information est toujours valable dans la mesure où les services fonctionnent à l'initiative de l'utilisateur. Rappelons, toutefois, que tout système télématique peut incorporer un ou plusieurs modèles de circulation de l'information. Dans le domaine des médias interactifs, qu'un système vidéotex se limite ou non à la consultation de pages d'informations par un utilisateur, comprenne ou non des transactions commerciales ou même l'organisation de référendums ou de sondages d'opinion électroniques, la saisie de données constituera de toute façon un problème. Comme cela apparaît plus loin, l'une des caractéristiques des médias interactifs est que leur utilisation entraîne la collecte et l'enregistrement de données à caractère personnel.

A un niveau général, la notion de «médias interactifs» implique une relation triangulaire: un utilisateur de services, un fournisseur de services et un transporteur. Toutefois, il faut reconnaître qu'il peut y avoir des partenaires additionnels à cette relation, par exemple les producteurs de l'information mise à la disposition des fournisseurs de services. En outre, il peut arriver que le fournisseur de services soit également le transporteur comme c'est le cas lorsque les PTT elles-mêmes ou des sociétés de câbles privées constituent et gèrent des bases de données centrales.

Si l'on réduit la relation à ses parties constituantes, les caractéristiques suivantes peuvent être identifiées:

i. L'utilisateur

Ce peut être un individu ou une entreprise privée ou publique. Toutefois, étant donné que notre cadre de travail concerne les données à caractère personnel des personnes physiques, l'accent est mis sur l'individu uniquement. Bien que son importance

commerciale soit évidente, le rapport ne traite pas de l'accès anonyme aux systèmes videotex, c'est-à-dire les cas où, par exemple, une base de données est interrogée par un tiers (un agent de voyage, une banque) à la demande d'un individu. En sa capacité d'utilisateur, ce dernier peut avoir accès aux services suivants:

a. Banques de données publiques ou privées qu'il peut consulter afin d'obtenir des informations, par exemple: la recherche documentaire, l'information sur les horaires, la météo, la Bourse, les programmes de cinéma, etc. Plus d'une centaine de milliers de pages-écrans peuvent être disponibles au niveau central dans un système videotex sans parler des possibilités de se connecter à d'autres bases de données décentralisées;

b. Télé-achat, il existe toute une gamme de services;

c. Banque électronique, une série de transactions financières est possible;

d. Réservations (trains, places de théâtre, vacances);

e. Réaction du public à des émissions;

f. Sondage électronique sur certains problèmes;

g. Demande de programmes de télévision;

h. Télétraitement;

i. Jeux électroniques ;

j. etc.

En ce qui concerne les formes d'intervention mises en oeuvre par l'individu pour déclencher le «dialogue» ou «l'interaction» ou, dans certains cas, «la consultation unilatérale» lorsque la banque de données à laquelle on accède demeure inchangée, il faut considérer le cadre de la communication entre l'usager et le fournisseur.

Premièrement, la télédistribution bilatérale utilisant soit les lignes de téléphone ordinaires ou des lignes louées, soit un câble privé (coaxial, fibres optiques), soit un satellite permet à l'individu disposant d'un téléviseur spécialement équipé (par exemple, d'un modem et d'un décodeur) d'accéder à une variété d'activités commerciales, de ventes au détail et de sources d'information. Le raccordement d'un micro-ordinateur à un téléviseur apporte une intelligence considérablement accrue aux possibilités interactives des systèmes bilatéraux. De plus, un ordinateur personnel équipé d'un écran et utilisant des lignes téléphoniques publiques ou privées peut également permettre des liaisons interactives avec un fournisseur sans le besoin d'un téléviseur traditionnel.

ii. Le fournisseur

Tout en se rappelant que les phénomènes examinés ne nécessitent pas obligatoirement la fourniture d'un service (par exemple, la fourniture d'informations où la conclusion d'un contrat dans le cadre du système de télé-achat, etc.) puisqu'il est possible pour

l'usager lui-même de fournir directement l'information (par exemple, en réponse à un sondage électronique par le biais d'un téléviseur spécialement adapté ou de tout autre terminal approprié), le prestataire de services peut être un organisme public ou privé fournissant des informations à partir de bases de données publiques ou privées, de détaillants, de banques, de sociétés de télévision par câble, etc.

iii. Le transporteur

Le transporteur est le moyen de télécommunication entre l'usager et le prestataire de services (il peut également être prestataire de services). Il peut relever du secteur public ou privé, ou, comme dans certaines économies, du secteur privé avec un certain contrôle de la part de l'Etat. Le lien entre l'usager et le prestataire peut être effectué de différentes façons: utilisation de lignes téléphoniques ordinaires ou de lignes louées, du câble public ou privé, ou de satellites,

4.2. Situation dans les Etats membres et réglementations existantes ou envisagées

Une analyse de la situation dans les différents Etats membres du Conseil de l'Europe permet de dresser le tableau suivant en ce qui concerne l'utilisation des systèmes interactifs et le cadre réglementaire envisagé.

Autriche

Il existe déjà des systèmes de circulation des données entre un abonné et une banque de données (ordinateur central) notamment par vidéotex (qui en Autriche fonctionne en tant que service public de vidéotex). Il faut souligner cependant que le système vidéotex autrichien en est encore au stade expérimental; des travaux préparatoires ont néanmoins déjà été effectués en vue d'élaborer une loi sur le vidéotex qui contiendra des dispositions sur la protection des données et constituera la base de l'organisation effective du service de vidéotex. Ce pas sera vraisemblablement franchi prochainement.

Le service vidéotex autrichien est organisé en partie de manière anonyme, évitant ainsi la mise en mémoire de données à caractère personnel.

En Autriche, par «médias interactifs», on entend également les unités auxiliaires privées (terminaux et modems) branchées sur les lignes téléphoniques, et qui permettent à un abonné d'avoir accès à des banques de données par l'intermédiaire des réseaux publics de données existants, utilisant le réseau téléphonique public et des terminaux privés.

Belgique

Le service vidéotex interactif de la Régie des télégraphes et des téléphones (RTT) a été inauguré le 27 mars 1986. L'option retenue par ce pays est de développer prioritairement le vidéotex professionnel. Dans un premier temps, le service vidéotex sera accessible au moyen de 300 portes permettant de desservir de 3000 à 6000 utilisateurs. Une extension à 600 portes pour une capacité totale de 6000 à 10000 utilisateurs est prévue.

Un arrêté ministériel définissant les conditions d'usage et les tarifs est en cours d'élaboration et devrait être publié bientôt. Les principes suivants devraient être exprimés dans cet arrêté:

- le serveur est responsable du contenu des données;

- la RTT assume la responsabilité du transporteur;

- la RTT assure également la facturation et conserve à cet effet les données nécessaires pendant environ six mois.

France

Orienté à ses débuts vers l'annuaire électronique, le Minitel offre maintenant toute une série de services interactifs (service télébancaire, achat à domicile, accès à des bases de données, jeux, etc.) par l'intermédiaire du monopole public des PTT. Ce terminal permet à l'utilisateur d'accéder à des bases de données décentralisées afin d'obtenir des services à travers des «portes» fournies par le réseau de commutation de paquets, Transpac. L'utilisateur peut également se connecter à des bases de données outre-mer par le biais de Telenet, auquel il peut être raccordé par la porte internationale contrôlée par les PTT.

Deux textes concernent les problèmes de protection des données posés par les médias interactifs : la loi du 6 janvier 1978 sur l'informatique et les libertés et la loi du 29 juillet 1982 sur la communication audiovisuelle.

La CNIL a joué un rôle influent en attirant l'attention des PTT sur la nécessité de se pencher sur la question de la protection des données. Conséquence des décisions de la CNIL, les PTT ont dû, par exemple, introduire des dispositions sur la protection des données en ce qui concerne la facturation détaillée du téléphone et les automates d'appel. En ce qui concerne le vidéotex interactif, un système de tarification unique, permettant d'assurer la protection des données («système kiosque»), a été introduit.

République Fédérale d'Allemagne

Un système de vidéotex (Bildschirmtext) fonctionne depuis juin 1984, les services transitant à travers la Deutsche Bundespost, qui possède un monopole public, vers des utilisateurs disposant d'un téléviseur spécialement adapté ou de terminaux à domicile. Outre la fourniture de dizaines de milliers de pages d'informations, le Bildschirmtext offre également une large gamme de services en permettant à l'usager d'avoir accès à des bases de données décentralisées à travers des portes dans le réseau. Les réglementations actuelles relatives aux télécommunications en République Fédérale d'Allemagne obligent la Deutsche Bundespost à protéger les données à caractère personnel au sein du service Bildschirmtext. Ces réglementations soulignent que «le droit à l'information, à la rectification, au blocage et à l'effacement des données à caractère personnel doit être affirmé vis-à-vis des fournisseurs ou des abonnés concernés». Un projet plus détaillé de protection des données est envisagé. La loi fédérale et les lois des Länder fournissent également un cadre réglementaire, de même que le traité sur le vidéotex interactif établi entre les Länder et le Gouvernement fédéral.

Irlande

Certains systèmes sont déjà en service et d'autres sont envisagés, en particulier dans le domaine du vidéotex, dans le secteur privé ou public, par exemple:

- Agrilive fournit des informations à la communauté agricole;

- Cognotec fournit des informations financières;

- Patric fournit des informations bibliographiques et en matière d'environnement.

De plus, la quasi-totalité des systèmes interactifs disponibles à l'échelon international ou des bases de données réelles est accessible aux utilisateurs irlandais. Il n'y a pas de réglementation particulière sur la protection des données. Une loi sur la protection des données a été promulguée en 1988.

Pays-Bas

Un grand nombre de projets fonctionnent actuellement dans ce domaine. Depuis quelques années, les PTT offrent un service interactif de vidéotex (Viditel) qui utilise le réseau de communication des PTT avec un équipement spécial vidéotex. Ce service est destiné au public ainsi qu'à des groupes d'usagers. Indépendamment du Viditel, il y a quelques douzaines de services vidéotex pour des groupes et un petit nombre de services privés de télé-achat. Divers types de services d'information, de réservation et de télé-achat sont désormais opérationnels à Limbourg dans le cadre d'une expérience à grande échelle utilisant des équipements bilatéraux de câble.

L'introduction et l'utilisation de ces services n’ont pas nécessité de réglementations spéciales. La protection juridique est assurée par des obligations réglementaires et contractuelles, par exemple, par les dispositions figurant dans le contrat Viditel au sujet du caractère confidentiel des informations sur les usagers.

Une loi sur la protection des données a été finalement adoptée en décembre 1988.

Norvège

Les médias interactifs ont été introduits dans certains secteurs en Norvège. Il existe, depuis quelque temps, une base de données juridiques qui couvre toutes les lois, tous les règlements et tous les répertoires de jurisprudence de la Cour suprême. Cette base de données est accessible au grand public mais, bien entendu, elle est essentiellement utilisée par des juristes et des organismes publics. Certains journaux et certaines agences de presse mettent leurs archives électroniques à la disposition du public. Pour ce faire, les journaux doivent se procurer une autorisation auprès de l'inspection des données. Ce service a fixé des règles à cet égard, par exemple certains types d'informations ne seront plus mis à la disposition du public sept ans après la date de publication.

La Norvège possède aussi quelques systèmes vidéotex. Le service Telecom a ouvert récemment au public son service vidéotex après une longue période expérimentale. Il est trop tôt pour dire dans quelle mesure ce système sera utilisé. Un autre système est

envisagé par une société d'information en matière de crédit, en coopération avec une banque. Ces sociétés souhaitent proposer des informations en matière de crédit, des informations économiques et un service de nouvelles à l'intention des abonnés. En outre, certains des journaux les plus importants envisagent de créer des systèmes proposant à leurs abonnés des nouvelles et d'autres informations, telles que des informations sur les entreprises. Certaines sociétés de traitement de données souhaitent aussi s'introduire sur ce marché.

Il y a actuellement, semble-t-il, une grande activité dans ce domaine en Norvège, mais la plupart des systèmes en sont seulement au stade de la conception et il semble que beaucoup n'ont pas été achevés pour la date prévue. Il faut donc attendre pour voir combien fonctionneront à l'avenir.

Jusqu'à présent, aucune législation spéciale n'a été adoptée dans ce domaine. La législation qui couvre, dans une certaine mesure, ce sujet est la loi relative aux registres de données à caractère personnel du 9 juin 1978, appliquée par l'inspection des données. Cette loi concerne essentiellement les registres de données à caractère personnel et elle couvre les systèmes en question dans la mesure où des registres de données à caractère personnel sont constitués.

Espagne

Un service de vidéotex (Ibertex) a été mis en service en février 1987; la Compagnie téléphonique nationale espagnole (Telefónica) fournira l'infrastructure de télécommunication. Des projets de «déréglementation», de Telefónica sont en cours. En dehors de la mise en place des circuits et de leur entretien, la seule intervention de Telefónica consistera à percevoir les redevances pour l'utilisation du service téléphonique ou du réseau lberpac pour bénéficier d'un service vidéotex. L'Association des fournisseurs d'informations est convenue de garantir, notamment, «le secret des données et de la vie privée des usagers».

Suède

Les usagers du vidéotex ne cessent d'augmenter en nombre en Suède, la progression étant la plus rapide dans le secteur des entreprises; l'usage du vidéotex gagne également du terrain dans les ménages. Pour leur part, de nombreuses banques se sont dotées d'un système télébancaire très complet faisant appel au vidéotex. Certains bureaux de poste disposent aussi désormais de terminaux permettant de réserver des places de théâtre, etc. En revanche, s'il est peu probable que des particuliers se servent déjà des «médias interactifs», bon nombre «d'agents de l'information» ont recours au vidéotex pour s'acquitter de leur fonction de «garçon de course électronique». Ces derniers sont en général en mesure de fournir des informations provenant de différentes sources, au choix du destinataire.

Aucune réglementation spéciale n'a été encore établie. La collecte, l'enregistrement et l'utilisation de données à caractère personnel par le biais du vidéotex sont couverts par la loi sur la protection des données.

Suisse

Le principal système interactif utilisé en Suisse est le vidéotex mais l'interrogation à distance d'une base de données peut aussi se faire par l'intermédiaire du télex. En outre, le service support Telepac offre à n'importe quel usager de ce service la possibilité de dialoguer avec des bases de données, s'il est équipé de terminaux adéquats. Telepac offre donc un support pour des systèmes interactifs. Les PTT mettent à disposition l'infrastructure technique nécessaire. En général, les bases de données sont privées. Le vidéotex fait l'objet d'un instrument juridique spécial qui, toutefois, ne contient pas de disposition sur la protection des données. Le projet de loi fédéral sur la protection des données ne contiendra probablement pas de dispositions spécifiques sur le vidéotex.

Royaume-Uni

La Compagnie britannique de télécommunications (British Telecom) offre un système vidéotex appelé Prestel, qui nécessite des téléviseurs spécialement équipés ou des terminaux d'ordinateurs reliés, par l'intermédiaire du réseau téléphonique, à une base de données qui peut offrir des services télébancaires, de réservations de voyages, de réservations pour le théâtre, de télé-achat, ou permet l'accès à des banques de données spécialisées, etc. Il n'existe pas de réglementation spéciale sur la protection des données en dehors des principes généraux de protection des données figurant dans la loi sur la protection des données. La Compagnie British Telecom, transporteur privé, fait l'objet d'un contrôle réglementaire en vertu de la loi sur les télécommunications qui impose la sauvegarde du secret de l'information transportée entre l'utilisateur et le fournisseur.

4.3. Analyse des problèmes de protection des données et solutions éventuelles

Du point de vue de la protection des données, la principale préoccupation concerne l'utilisation secondaire éventuelle des informations à caractère personnel révélées par les individus chaque fois qu'ils utilisent un système interactif. Une des caractéristiques des systèmes interactifs est que leur utilisation crée des données à caractère personnel: par exemple, X a acheté un certain article, regardé tel film, transféré une certaine somme d'argent, joué avec tel jeu électronique, répondu d'une certaine façon à un sondage électronique, etc. L'information est transportée par le biais du réseau de télécommunications vers les destinataires de manière que le service demandé puisse être fourni. Les données communiquées par l'usager sont enregistrées par le prestataire de services pour la fourniture du service lui-même et à des fins de facturation. Le transporteur enregistre également l'information sur l'usager à des fins de facturation (notamment temps passé sur le réseau, numéro d'appel du service, etc.). Lorsque le transporteur est le gérant de la base de données ou le fournisseur du service, ce qui est souvent le cas pour les systèmes publics de vidéotex ou les sociétés de télévision par câble, un important fichier d'informations se trouve être entre les mains d'une seule et même entité. En d'autres termes, le modèle de circulation de l'information à tendance à correspondre à celui de l'enregistrement et c'est à ce niveau que des problèmes de protection des données se posent. Il existe donc un risque que les données collectées pour les besoins d'un service particulier soient mises à la disposition de tiers afin d'être utilisées à des fins entièrement différentes. En d'autres termes, il est possible de commercialiser et de détourner les données à caractère

personnel induites par l'utilisation du système, et des utilisations secondaires de l'information peuvent intervenir sans que l'utilisateur en ait connaissance.

La question devient plus complexe lorsque l'utilisation secondaire est examinée en termes de profil individuel. Une image informatisée de l'usager peut en effet être établie, à partir des révélations faites par lui-même: ses goûts en matière de littérature, de produits de consommation, de films, son intelligence peut être évaluée par le biais de sa participation à certains puzzles électroniques. Le profil lui-même peut être commercialisé mais l'élément de surveillance ou de contrôle des utilisateurs qu'une telle technique permet est peut-être une éventualité plus alarmante. Compte tenu de ce qui a été dit, lors de la discussion sur la télémétrie, en ce qui concerne la possibilité de placer des détecteurs sensibles sur des systèmes interactifs de télévision, il est possible d'effectuer un contrôle encore plus complet par le biais de la télévision interactive puisque les mouvements de l'usager vont être également enregistrés dans le système (lorsqu'il quitte sa maison, lorsqu'il rentre).

Le fait que le transporteur soit un organisme contrôlé par l'Etat ou une entreprise privée ajoute une autre dimension au problème. Bien que, dans les deux cas, les données soient collectées à des fins de facturation, il ne faut pas oublier que la facture est établie à partir d'un individu identifiable appelant des services particuliers identifiables à certaines occasions et pendant un certain laps de temps. Un lien étroit entre le transporteur et l'administration est susceptible d'augmenter les inquiétudes en ce qui concerne les possibilités de surveillance des systèmes interactifs.

L'utilisateur est en train de créer de façon inconsciente le plus grand répertoire de données à caractère personnel de l'histoire de l'humanité (Flaherty). Etant donné qu'il n'est pas en mesure d'apprécier totalement les conséquences de l'utilisation des systèmes interactifs en ce qui concerne les informations divulguées, un problème se pose quant au caractère loyal des procédures de collecte des données. A quoi l'utilisateur consent-il lorsqu'il communique les données? Comment peut-il exprimer ce consentement? Comment peut-il suivre l'utilisation faite des données le concernant? Ces problèmes sont liés au manque de transparence des systèmes, en ce sens que les activités et responsabilités des différents acteurs impliqués ne sont pas clairement définies - le prestataire peut également être le transporteur, recueillant et traitant des données pour les services fournis ainsi que pour la facturation. Les informations relatives à l'utilisateur peuvent faire l'objet de différents «fichiers» - fichiers concernant le trafic, fichiers concernant les données de facturation et fichiers sur les demandes du consommateur. Qui gère tel fichier et à quelles fins? Le manque d'articulation entre les droits et les devoirs des différents acteurs impliqués empêche l'utilisateur de contrôler l'utilisation faite de ses données.

L'analyse comparative des différentes approches adoptées pour résoudre les problèmes de protection des données posés par les médias interactifs donne à penser qu'une loi nationale sur la protection des données n'est peut-être pas suffisamment efficace pour traiter de tous les problèmes. Les législateurs sont néanmoins d'accord sur un point, à savoir que dans la mesure où les médias interactifs donnent lieu à la collecte, à l'enregistrement et au traitement de données à caractère personnel, les normes générales et les pouvoirs de surveillance des différents organes de contrôle énumérés dans les lois nationales sur la protection des données sont applicables. Le succès de l'organe chargé de contrôler les abus dans ce domaine dépendra dans une

large mesure de sa capacité à adapter les principes généraux de la protection des données aux particularités des médias interactifs.

Cette approche n'est pas sans poser de problèmes, l'un des plus importants étant que beaucoup de lois, en particulier celles adoptées dans les années 70, n'ont pas été conçues dans la perspective des médias interactifs et des problèmes y relatifs. Ceci est vrai pour les nouvelles technologies en général.

Il paraît donc souhaitable de traiter les problèmes des médias interactifs en adoptant une approche sectorielle. Le videotex, par exemple, a déjà fait l'objet d'une réglementation particulière (c'est-à-dire, en dehors du cadre de la législation générale Sur la protection des données) en République Fédérale d'Allemagne. L'expérience montre qu'il est possible de trouver des solutions particulières, basées sur les principes généraux de la protection des données, pour les problèmes spécifiques décrits ci-dessus. En se basant sur les exemples nord-américain et européen (en particulier la République Fédérale d'Allemagne) dans le domaine du vidéotex, il semblerait utile que tout nouveau projet de réglementation se concentre sur les points suivants:

i. consentement de l'utilisateur préalablement à l'installation d'un système vidéotex dans sa résidence;

ii. seules les données à caractère personnel qui sont nécessaires à des fins de facturation ou de service devraient être collectées et enregistrées;

iii. la vente, la divulgation ou une utilisation ultérieure des données ne devraient être possibles qu'avec le consentement éclairé de l'utilisateur ou que si cela est prévu par la loi;

iv. la sécurité et la confidentialité des données à caractère personnel enregistrées devraient être assurées notamment au moyen de techniques de cryptage, de la carte à mémoire ou du changement de mots de passe;

v. des périodes strictes de conservation des données devraient être prévues;

vi. les droits de l'utilisateur (accès, suppression et rectification) devraient être définis et celui-ci devrait être informé de leur existence et des moyens de les exercer;

vii. la législation générale sur la protection des données, lorsqu'elle existe, devrait fournir le cadre réglementaire général.

Pour ce qui est de la mise en oeuvre de ces principes dans les Etats membres, le recours à une loi spécifique paraît être le moyen le plus évident. Toutefois, en s'inspirant de l'expérience allemande, il est également possible d'intégrer ces principes dans le cadre réglementaire général sur les télécommunications.

On peut en outre noter que l'autoréglementation a un rôle à jouer dans ce domaine. L'expérience nord-américaine illustre en particulier les possibilités offertes à l'industrie du vidéotex dans le secteur privé pour soumettre ses membres à des codes de conduite ou de pratique. Cette approche semble particulièrement adaptée à l'environnement de «déréglementation» qui caractérise le domaine de la télévision

interactive par câble. Toutefois, l'autoréglementation devrait être considérée comme un complément éventuel à la législation existante sur la protection des données et de telles initiatives devraient prendre en compte ce cadre plus général. Dans ce contexte, on pourrait envisager que les organes de surveillance établis conformément aux lois sur la protection des données agissent eux-mêmes comme ultimes arbitres de l'efficacité des codes de conduite proposés.

On peut également imaginer une solution intermédiaire entre une disposition prévue par la loi et l'autoréglementation; les exemples nous viennent une fois de plus de certains Etats américains. Bien que cette approche ne soit pas adaptée à un système public de videotex, on pourrait envisager, dans le domaine de la télévision interactive par câble, un contrôle des fournisseurs de services ou des transporteurs par le biais d'un contrat ou d'une licence, au moment de la délivrance d'une autorisation officielle d'exploiter un réseau de télévision par câble dans une région déterminée.

Enfin, outre les propositions ci-dessus, il conviendrait d'étudier de manière plus approfondie une solution qui apporterait une réponse totalement différente et élégante à ces problèmes de protection des données: la technologie videotex permet de faire en sorte que l'usager fasse appel aux services, banques de données, etc., de manière anonyme, sans qu'aucune donnée de caractère personnel ne soit mise en mémoire par le prestataire de services ou le transporteur. De cette manière, on évite dès le départ bon nombre des risques connus. Ce système a, par exemple, déjà été mis en place en Autriche pour l'accès aux services gratuits par l'intermédiaire du videotex (BTX). A l'avenir, la sophistication croissante de la carte à mémoire devrait permettre d'étendre le videotex anonyme à l'accès aux pages payantes. On peut concevoir des dispositions législatives ou réglementaires rendant obligatoire l'application de cette nouvelle technologie dès que le progrès technique le permettra.

5. Courrier électronique

5.1. Description des services et caractéristiques techniques

Le terme «courrier électronique» est relativement clair et ne nécessite pas une description approfondie. Il s'agit du modèle conversationnel (échanges d'informations entre des individus) de circulation de l'information, caractérisé par l'égalité de statut des participants.

Selon une définition large, les systèmes de courrier électronique consistent en un terminal et un clavier, capables de transmettre des messages codés par l'intermédiaire du réseau téléphonique auquel le ou les destinataires sont reliés. D'autres services peuvent être inclus: la boîte à lettres électronique où le destinataire trouvera les messages enregistrés et envoyés; la mise en fiche électronique des messages envoyés ou reçus pendant une période donnée.

Les systèmes de courrier électronique peuvent également concerner la transmission d'enregistrements phoniques (messagerie vocale).

Rappelons enfin que les systèmes videotex décrits au chapitre précédent peuvent comprendre une forme de courrier électronique.

5.2. Situation dans les Etats membres et réglementations existantes ou envisagées

La plupart des Etats membres du Conseil de l'Europe ont développé des systèmes de courrier électronique, publics ou privés. Pour l'instant, ces systèmes concernent davantage les entreprises ou l'administration et ne concurrencent pas encore le service postal, qui reste un moyen fiable et peu onéreux de transporter le courrier. On peut distinguer deux types de messagerie: les messageries internes d'entreprises qui utilisent les réseaux internes de ces entreprises; et les messageries interentreprises qui relèvent quant à elles du service public (c'est le cas dans la plupart des pays européens) ou utilisent les services d'un transporteur privé.

En Belgique, un système public de messagerie électronique écrite a débuté en mai 1985. Ce service est exploité par la Régie des télégraphes et des téléphones, qui dispose d'un monopole dans ce domaine. Un arrêté ministériel fixe les modalités de tarification. Des systèmes de messagerie électronique ont d'autre part été mis en place dans différents ministères (Bistel).

En République Fédérale d'Allemagne, des services expérimentaux de courrier électronique (Telebox) et de transmission d'enregistrements phoniques (Sprachspeicherdienst) ont été mis en place. Une réglementation relative à ces services est en cours d'élaboration. Elle prévoit, en ce qui concerne le service Telebox, que chaque récepteur est protégé par un code alphanumérique (de six à trente caractères). Les messages particulièrement confidentiels peuvent être protégés additionnellement par un code spécifique de vingt caractères au maximum. Lors de chaque accès par l'usager, le système reproduit automatiquement la date et l'heure du dernier accès, afin de l'informer d'un éventuel accès non autorisé. Lorsqu'il y a trois essais infructueux pour accéder à un récepteur le système est coupé. En ce qui concerne le service d'enregistrements phoniques, la protection contre l'accès non autorisé au récepteur (Sprachbox) est garantie par les mesures suivantes: identification à sept caractères de la station sélectionnée; mot de passe individuel ayant au maximum huit caractères.

En Irlande, le Conseil national des télécommunications offre un service de courrier électronique dans le cadre de son réseau commuté. En outre, le service postal national dispose d'un tel système depuis la fin de 1986. Le cas échéant, les données électroniques peuvent être imprimées sur papier et délivrées par le service postal.

Aux Pays-Bas, les PTT ont récemment lancé un service public de courrier électronique (Memocom), utilisant les réseaux existants du téléphone et du traitement des données. Plusieurs entreprises privées possèdent en outre leur propre système interne de courrier électronique. On envisage d'autre part la possibilité d'introduire un tel système dans l'administration. Dans ce pays, la communication au moyen du téléphone ou du télégraphe est protégée par la Constitution. La communication des données est régie par les dispositions de l'ordonnance de 1982.

Au Royaume-Uni, des services de messagerie électronique tant publics que privés sont largement utilisés. Le service public le plus connu est le Telecom Gold de British Telecom, qui fournit non seulement l'équipement de base nécessaire à l'enregistrement et à la transmission des messages, mais aussi un service de télex et des passerelles vers les systèmes de vidéotex. Telecom Gold connaît un développement rapide et

double chaque année le nombre de ses utilisateurs. De nombreux grands organismes des secteurs public et privé possèdent par ailleurs leurs systèmes propres de messagerie électronique, dont certains sont reliés aux réseaux internationaux.

5.3. Analyse des problèmes de protection des données

Les problèmes de protection des données ne sont pas fondamentalement différents selon que l'on se trouve en présence de messageries internes d'entreprises ou de messageries externes, c'est-à-dire utilisant le réseau téléphonique ordinaire (c'est le cas dans la plupart des pays européens) ou nécessitant d'utiliser les moyens de communication offerts par un transporteur.

Dans un cas et dans l'autre, il s'agit d'éviter les accès non autorisés, d'assurer avec certitude l'identification de l'expéditeur, de dater avec précision l'envoi et de garantir l'intégrité du contenu des messages. Le droit de la preuve et ses possibles évolutions peuvent être cités dans ce contexte. Toutefois, il semble que ce problème ne soit pas différent de celui qui se pose en relation avec les autres technologies informatiques (preuve de l'identité de l'utilisateur et du destinataire, preuve du contenu du message, valeur de l'accusé de réception éventuellement délivré, etc.).

En matière de sécurité, la question de la gestion des mots de passe se pose. Il a été en effet constaté qu'il peut être dangereux de laisser à l'utilisateur le choix du mot de passe. L'expérience prouve que celui-ci choisira généralement une information assez facilement reconstituable par des tiers. L'information et l'éducation des utilisateurs paraissent donc souhaitables.

Les messages circulant dans un réseau de courrier électronique peuvent contenir toutes sortes de données et faire l'objet d'un fichier. Des conflits de lois possibles peuvent éventuellement intervenir. En effet, les messages doivent-ils d'abord être considérés comme des lettres, auquel cas la législation sur le secret de la correspondance s'applique? Ou bien faut-il leur appliquer les lois sur la protection des données, puisqu'il s'agit de données nominatives sur support magnétique? Ce problème est important puisque aux termes de ces lois, une personne dispose d'un droit d'accès aux informations la concernant.

On peut considérer toutefois que le message est une lettre et reste à ce titre confidentiel. La personne qui transmet le message est mai7tre de son contenu et peut y inclure des données à caractère personnel concernant d'autres personnes si elle le souhaite. Si, pour des raisons d'archivage ou autres, ces messages font l'objet d'un fichier, on ne peut appliquer à ces fichiers les dispositions des lois sur la protection des données en matière de droit d'accès ou de rectification sans remettre en cause le droit au respect du secret de la correspondance, garanti par l'article 8 de la Convention européenne des Droits de l'Homme. Le fait que la transmission du message se fasse de façon électronique ne change rien au principe du secret de la correspondance. Le problème réside en fait autre part; il s'agit avant tout d'assurer la sécurité des messages.

Il apparaît en outre nécessaire de définir la responsabilité du maître du réseau. A l'heure actuelle, il ne semble pas que les législations existantes permettent d'engager la responsabilité du maître de réseau, excepté dans certains pays en cas de faute lourde. Celui-ci doit en effet garantir la confidentialité et la sécurité des messages.

Enfin, le courrier traditionnel bénéficie dans la plupart des pays d'une garantie de secret inscrite dans la loi. En matière de courrier électronique, cette garantie n'est plus aujourd'hui clairement définie. Il paraît important que les PTT offrent au courrier électronique les mêmes garanties que celles accordées au courrier traditionnel. C'est une condition du développement de ces services, notamment au niveau domestique.

On peut déduire de ces réflexions que deux points paraissent essentiels dans le domaine du courrier électronique:

1. le respect de la confidentialité des messages, qui devrait être garanti par la loi au même titre que pour le courrier traditionnel;

2. le développement de mesures techniques pour assurer une meilleure sécurité des messages. Parmi ces techniques, on peut citer: le datage automatique, le séquencement des messages, le chiffrement et l'émission d'accusés de réception.

6. Aspects communs des problèmes de protection des données

Chacune des technologies examinées peut présenter un certain nombre de problèmes de protection des données. Les normes de protection des données existantes sont-elles en mesure de résoudre ces problèmes, ou est-ce que les concepts sur lesquels elles sont basées font référence à une période technologique dépassée, ce qui les empêche effectivement de résoudre les nouveaux problèmes? Etant donné l'influence des dispositions de la Convention pour la protection des données sur l'élaboration des normes de protection des données (élaboration elle-même influencée par l'approche du législateur dans les années 70), il est intéressant d'examiner si les concepts et la terminologie utilisés dans la Convention, au vu des nouveaux problèmes qui se posent, sont encore pertinents et valables. Alors que les analyses faites dans les chapitres précédents de ce rapport visaient des problèmes spécifiques ainsi qu'une présentation comparative des moyens de s'attaquer à ces problèmes, le présent chapitre a davantage pour objectif d'évaluer l'impact général sur le cadre normatif élaboré pour réglementer le traitement automatisé des données à caractère personnel.

Les conclusions de cet exercice ne devraient pas être considérées comme s'appliquant spécifiquement aux médias interactifs, à la télémétrie et aux systèmes de courrier électronique et comme n'ayant aucun lien avec les autres applications technologiques au-delà des limites des exemples de départ. Au contraire, le législateur est invité à s'interroger par-delà les exemples concrets et à examiner les applications télématiques auxquelles il n'est pas fait référence dans ce rapport, par exemple systèmes de traitement de texte, carte à mémoire, systèmes experts, etc., qui créent des possibilités accrues de traitement de données à caractère personnel collectées et enregistrées consécutivement à 1'utiiisatioii individuelle d'un système ou du fait du contrôle effectué par un système. Pour illustrer ce propos, disons que, bien que la confidentialité et la sécurité des données soient traitées plus tard du point de vue des problèmes posés par la mise en oeuvre de l'article 7 de la Convention sur la protection des données dans le domaine de la télémétrie, des médias interactifs et des systèmes de courrier électronique, les questions soulevées dans ces domaines concernent en général les données à caractère personnel qui transitent dans les réseaux ou qui sont enregistrées dans ces réseaux, quelle que soit la technologie utilisée. De même, les défis lancés au principe de base concernant la qualité des données figurant à l'article 5

devraient être considérés comme ayant une application plus large, allant au-delà des exemples et des solutions spécifiques qui sont décrits.

Il convient également de se rappeler les conclusions auxquelles le chapitre 2 avait abouti en ce qui concerne les tendances en matière de technologie: la banalisation de l'informatique qui fait que de plus en plus de personnes sont directement concernées par ces problèmes, par exemple en tant qu'utilisateurs; la tendance vers des systèmes de traitement distribué; les possibilités largement accrues de transmission des données; l'interconnexion des fichiers; et le caractère multifonctionnel des réseaux.

1. Article 2.a de la Convention - La définition des données à caractère personnel

Le moins que l'on puisse dire est que la quantité de données à caractère personnel qui sont en circulation s'est accrue de façon dramatique. On l'a vu au chapitre 2, la télémétrie, les médias interactifs et, dans une certaine mesure, les systèmes de courrier électronique sont utilisés au niveau domestique et permettent la collecte et l'enregistrement de données à caractère personnel de plus en plus nombreuses à travers des systèmes de traitement de données. Les informations enregistrées concernent dans une large mesure l'individu en tant qu'utilisateur de services, la consommation énergétique d'un ménage donné, le temps passé sur une ligne de télécommunication, etc. Mettre en relation les données avec une personne physique identifiée ou identifiable pose donc relativement peu de problèmes. Un problème se pose éventuellement au niveau de l'utilisation collective d'un service télématique, notamment un foyer où les informations collectées et enregistrées reflètent l'activité du groupe. Par exemple, l'utilisation commune d'un mot de passe par les membres d'une famille, pour accéder à Lin système de courrier électronique ou au vidéotex, ou le relevé de la consommation énergétique d'un foyer entraînent un enregistrement de données caractérisant l'activité du groupe aux dépens de l'utilisation individuelle, ce qui ne permet pas à l'utilisateur individuel de «situer» ses propres données. D'un certain point de vue, il s'agit d'un problème de protection du consommateur, qui peut être résolu par le biais de la technique de la facturation détaillée dans le cas du vidéotex et du courrier électronique. D'un autre point de vue, il se pose un problème de protection de la vie privée du fait que l'individu est lié involontairement à l'attitude du groupe auquel il appartient. Il existe une autre dimension au problème: les droits du groupe même. Les données rassemblées sur le groupe peuvent empêcher une identification des individus qui le constituent mais dans la mesure où les données enregistrées sur le groupe peuvent être utilisées pour prendre des décisions ou porter des jugements de valeur qui affectent finalement à la fois le groupe en tant que tel et, nécessairement, ses membres, un problème se pose quant à l'opportunité d'inclure dans un projet sur la protection des données la reconnaissance d'une protection de la vie privée du groupe. Toutefois, il se peut très bien qu'un tel problème ne remette pas en cause la définition des données à caractère personnel dans la Convention. Il serait préférable en fait d'analyser de tels problèmes à travers les moyens utilisés pour la collecte, les raisons de cette collecte et l'utilisation qui sera faite des données.

La notion de personnes identifiables peut également connaître des changements. La Convention n'avait pas pour objectif de couvrir l'identification des personnes au moyen de méthodes très sophistiquées. Toutefois, ce qu'on appelle une méthode sophistiquée dépend de l'état de la technologie. En résumé, ce qui n'était pas possible techniquement en 1970 peut l'être aujourd'hui. Et le temps passant, d'autres

possibilités d'identifier les individus parmi la masse anonyme ne manqueront pas d'apparaître.

On peut d'autre part se demander dans quelle mesure le concept de «données à caractère personnel» de la Convention tient compte des nouvelles possibilités d'enregistrer et de traiter les images, les sons et les voix. Lorsque la télémétrie permet de numériser et d'enregistrer des photos de conducteurs automobiles pénétrant au centre de la ville, ou de consommateurs faisant la queue dans une banque, ou lorsque les systèmes de courrier électronique permettent d'enregistrer automatiquement la voix humaine, on est en mesure d'apprécier les nombreuses et différentes formes que les informations à caractère personnel peuvent revêtir et, partant, la nécessité d'apprécier ce phénomène dans le contexte le plus large possible. A nouveau, la définition de la Convention devrait être considérée comme suffisamment souple pour pouvoir couvrir ce type de problèmes. Ceci dit, il faut soigneusement réfléchir avant de venir à la conclusion que, puisqu'un traitement automatique de données à caractère personnel a lieu dans un contexte donné, le système de protection des données est de ce fait en cause à l'exclusion d'autres considérations. Il peut être parfois instructif d'examiner les limites à ce que constituent des données à caractère personnel lorsqu'on souhaite inclure certaines activités de traitement dans le cadre réglementaire de la protection des données. Par exemple, pour reprendre une question déjà discutée au chapitre 5, il est possible d'analyser les systèmes de courrier électronique en termes de traitement automatique et d'enregistrement de données à caractère personnel concernant des individus identifiables. Toutefois, le point de départ pour résoudre les problèmes consécutifs à l'utilisation de systèmes de courrier électronique peut très bien être trouvé dans les notions traditionnelles du secret de la correspondance, de la confidentialité du courrier, de l'interception non autorisée, plutôt que dans le concept de protection des données.

2. Article2.b - La définition d'un fichier automatisé

Le concept de «fichier automatisé» est considéré comme de très grande importance dans le domaine de la protection des données. Il contribue à la transparence et au contrôle des traitements automatiques de données dans la mesure où la personne concernée est informée de son existence, ce qui permet à cette dernière d'exercer ses droits d'accès, de rectification et d'effacements Il se peut, toutefois, que la notion de fichier, telle qu'utilisée dans la Convention, suggère un enregistrement et un traitement centralisés, ce qui ne correspond plus tout à fait à la nouvelle réalité de l'informatique répartie et des réseaux qui permettent aux données de se disperser tout en pouvant être reliées à volonté à travers la possibilité d'un dialogue d'ordinateur à ordinateur ou de terminal à ordinateur. Si un fichier de données est divisé en plusieurs sous-ensembles de données, une tâche inacceptable est imposée à la personne concernée qui est obligée de remettre ensemble les différentes pièces du puzzle y compris débrouiller le réseau avant de pouvoir véritablement parvenir à ses données. En réalité, l'exercice effectif du droit d'accès de la personne concernée disparaît, le contrôle individuel sur le traitement de ces données s'amenuise et la transparence diminue.

Ce phénomène pourrait être typique de toute organisation qui fonctionne selon le schéma suivant: un réseau local et différentes personnes qui extraient et traitent des données à caractère personnel à différentes parties du réseau. Les services publics

auxquels il est fait référence dans le domaine de la télémétrie, du courrier électronique et des médias interactifs - les PTT et les différentes compagnies de gaz, d'électricité ou d'eau, par exemple - peuvent répondre à une telle description de traitement réparti des données. En conséquence, il se peut très bien qu'au sein des PTT, un fichier de données contenant des données d'appel et des données de facturation soit difficile à localiser. En fait, il faudrait mettre en rapport une série de fichiers représentant les différentes utilisations faites par l'abonné des lignes téléphoniques, avant de connaître la somme des données à caractère personnel enregistrée par les PTT à des moments donnés.

Il paraîtrait nécessaire d'examiner la nécessité de pouvoir établir l'existence de ce qu'on pourrait appeler «un fichier logique», permettant de situer en dernier ressort, à travers des méthodes d'extraction, toutes les données dispersées dans le réseau à la suite d'un traitement et d'un enregistrement légitimes au sein d'une organisation donnée. De même, la transparence n'est plus assurée par le simple fait de connaître l'existence d'un fichier. Il serait donc souhaitable de rendre plus claire l'influence du réseau sur les opérations de traitement des données.

Les systèmes de courrier électronique, comme il a été dit auparavant, ont des caractéristiques spécifiques. Il est notamment inapproprié de considérer les messages numérisés, en attente dans le système pour être ramassés par le destinataire, comme «des fichiers de données», étant donné leur nature non structurée. Si cette conclusion peut ne pas être valable pour les fichiers contenant les données d'appel ou les fichiers contenant les données de facturation résultant de l'utilisation des médias interactifs ou de la télémétrie, elle est par contre valable en ce qui concerne les technologies autres que les systèmes de courrier électronique - les systèmes de traitement de texte, par exemple, se caractérisent plus par l'enregistrement de textes libres que par des ensembles structurés de données. Les difficultés qu'un tel système pose vis-à-vis du droit d'accès sont tout à fait évidentes.

3. Article 2.d - La définition du «maître du fichier»

Cette discussion est inévitablement liée aux considérations précédentes sur les fichiers de données. Les systèmes répartis de traitement des données impliquent une décentralisation du contrôle et des responsabilités et rendent difficile l'identification «de la personne ou de l'organe responsable en dernier ressort du fichier». On se rappelle que la Convention base les droits de la personne concernée sur la possibilité d'établir l'identité et la résidence habituelle ou le principal lieu de travail du «maître du fichier». Les systèmes de courrier électronique remettent immédiatement en question la validité de la notion de «maître du fichier» étant donné l'impossibilité d'étendre le concept de «fichier de données, aux messages électroniques. Néanmoins, il paraît essentiel d'adapter la notion de «maître du fichier» afin de prendre en compte le nouveau contexte technologique et de résoudre les problèmes de responsabilité lorsque quelque chose ne fonctionne pas dans les systèmes de courrier électroniques Si le terme «maître du fichier» n'est plus approprié, il serait peut-être souhaitable de parier de «maître du réseau ». En dehors du courrier électronique et des autres systèmes caractérisés par le modèle conversationnel de circulation de l'information, la notion de «maître du fichier» reste toujours valable si l'on prend en compte les facteurs mentionnés dans l'analyse sur les fichiers informatisés de données. En conséquence, dans un système de traitement réparti et décentralisé, une personne ou

un organe peut très bien être responsable en dernier ressort de «fichiers» particuliers si l'on se réfère aux derniers utilisateurs autorisés des données - est-ce que ce sont les PTT, une entreprise de télévision par câble, un fournisseur de services, ou alors une compagnie d'électricité? Même si le dernier utilisateur autorisé ainsi identifié - et pour cette raison il est essentiel que les rôles des différents acteurs impliqués dans un service télématique soient clairement communiqués à l'utilisateur - gère un système réparti de traitement de données, il devrait toujours être possible de le considérer comme contrôlant toutes les opérations de traitement sur un fichier donné et notamment comme étant le dépositaire de la totalité des données à caractère personnel situées dans un réseau - ce qu'on a appelé «fichier logique».

4. Article 5. a - Le principe de la collecte loyale et licite

Comme le montrent les analyses sur la télémétrie et les médias interactifs, les nouvelles technologies offrent de nouveaux moyens de collecter des données. L'individu ne fournit pas des informations en réponse à des questions posées par des tiers mais crée des données en dialoguant avec un système. Ses mouvements, sa consommation énergétique, sa présence physique, la façon dont il utilise un système, ses dialogues avec le système donnent naissance à des données - ce qui n'a peut-être pas été envisagé lorsque ce principe a été rédigé. Ce dernier est toujours valable, mais son intérêt diminue si on le considère exclusivement comme impliquant une interdiction en cas de tromperie ou de mauvaise interprétation. Il faudrait plutôt le considérer dans le contexte plus large d'un droit de contrôle sur l'information - c'est-à-dire le droit de l'individu de contrôler la quantité de données qui sont collectées à son sujet, de suivre l'utilisation faite de ces données et de rester à tous les stades conscient des différentes opérations qui sont effectuées sur ces données.

Les systèmes télématiques, qu'ils appartiennent aux modèles de la consultation (médias interactifs) ou aux modèles de l'enregistrement (télémétrie), se caractérisent par la collecte et l'enregistrement de données à caractère personnel, quelle que soit la distinction faite sur le caractère actif ou passif de la personne concernée vis-à-vis d'un système particulier. Même si l'analyse faite au chapitre 3 sur la collecte des données effectuée par un système de télémétrie prouve la nécessité de rendre la personne concernée plus consciente de ce qui se passe en réalité, on considère qu'un tel besoin de transparence existe également en ce qui concerne les systèmes transactionnels. La télémétrie et les médias interactifs soulèvent des problèmes communs - possibilité accrue de surveillance et de contrôle, utilisation secondaire et appréciation variable de ce qui se passe de la part des individus.

Si l'on veut que le principe de «collecte licite et loyale» s'applique, deux idées devraient être examinées i. la transparence, et ii. le consentement. Ces deux notions peuvent paraître complémentaires et peut-être serait-il préférable de parler de «consentement libre et éclairé de la personne concernée». Cette idée est la mieux traduite par l'obligation de rechercher le consentement de l'individu préalablement à l'installation d'un système électronique dans son foyer, à la fourniture d'informations sur ce qui se passe lorsque la technologie fonctionne, à la fourniture d'informations sur le potentiel de collecte de données du système, etc.

Ce que l'on appelle une procédure de collecte licite et loyale dépendra bien sûr du traitement. Comme on l'a vu au chapitre 3, la télémétrie a des applications en dehors

de la maison. Il est difficile de mettre en oeuvre le principe de «consentement libre et éclairé» pour la surveillance vidéo d'une foule, par exemple. Dans de tels cas, il serait plus approprié de rechercher une solution au niveau législatif avant que des données puissent être collectées. D'un autre côté, dans le contexte de l'emploi, la collecte de données sur les employés par le biais de la télémétrie devrait dépendre du consentement libre et éclairé des employés.

5. Article5.b - Le principe de finalité

Dans le domaine de la télémétrie, les données sont essentiellement collectées à des fins de facturation on a vu en effet que les systèmes télémétriques existants concernent principalement le relevé à distance de compteurs d'eau, d'électricité ou de gaz. Les données enregistrées devraient donc se rapporter à la personne elle-même nom, adresse, compte bancaire, etc.) ainsi qu'à sa consommation. A ce propos, on a vu que la fréquence de l'enregistrement des données sur la consommation pouvait représenter un danger pour la vie privée de l'individu concerné. Ainsi, en Norvège, on envisagerait de relever les compteurs individuels toutes les six minutes, ce qui aboutit en fait à une surveillance quasi policière des individus. La finalité même du traitement, à savoir le relevé de la consommation de gaz, d'électricité ou d'eau, ne justifie pas une telle fréquence d'enregistrement de données, même pour des besoins de gestion interne. Il paraît donc essentiel que, lors de la mise en place d'un système télémétrique dans le foyer d'un individu, celui-ci soit informé de la fréquence et du moment de l'enregistrement des données.

Dans le cas d'un système de surveillance, installé soit dans une maison individuelle, soit sur un lieu de travail, il importe que les données enregistrées soient effacées dans un délai raisonnable. De tels systèmes sont généralement installés pour des raisons de sécurité et les données enregistrées ne doivent pas être utilisées à d'autres fins: par exemple pour la surveillance des individus se trouvant sur le lieu de travail.

Pour ce qui est du premier cas envisagé, à savoir les relevés à distance de la consommation d'eau, d'électricité ou de gaz, les possibilités d'utilisations secondaires des données paraissent négligeables. On peut admettre, dans ce cas, une utilisation interne des données, par exemple, pour des besoins de gestion du service. Toutefois, s'il s'agit d'un service public, les données ne devraient pas pouvoir être communiquées à d'autres services que le service concerné.

Pour ce qui est de la surveillance à distance, les risques d'utilisation secondaire sont plus grands et il importe dans ce domaine que les finalités soient clairement spécifiées et respectées. Aucune utilisation secondaire de ces données ne devrait être envisagée.

Enfin, dans le domaine de la télémétrie en général, un délai de conservation maximal des données devrait être prévu.

C'est certainement dans le domaine des médias interactifs que les problèmes d'utilisation secondaire des données se posent le plus. Deux types de données sont collectés et enregistrés, les données permettant l'établissement d'une facture pour le service fourni et les données qui sont révélées et enregistrées lors de la consultation du service demandé par la personne. Ce sont ces dernières données qui peuvent révéler les goûts et les habitudes des personnes et qui sont susceptibles d’utilisation

secondaire. D'autres prestataires de services pourraient en effet avoir intérêt à posséder ces données pour des raisons commerciales. A ce stade, il convient peut-être de faire une distinction entre le transporteur et le fournisseur de services. Pour ce qui est du premier, il doit garantir une sécurité convenable lors de l'enregistrement et de la transmission des données. Les seules données que ce dernier peut collecter et enregistrer concernent uniquement l'établissement d'une facture pour le service rendu, à savoir le transport des informations. Le fournisseur, quant à lui, devrait s'abstenir de communiquer à des personnes étrangères les informations recueillies par la personne concernée ainsi que les questions posées par lui. On peut toutefois envisager une utilisation interne légitime de ces données par le fournisseur lui-même, pour des besoins de gestion. La vente de telles informations ou de listes de noms devrait être réglementée. Le consentement libre et éclairé de l'individu concerné devrait être prévu, le terme «éclairé» signifiant que la personne doit exactement savoir à quoi elle s'engage en acceptant que son nom soit divulgué à d'autres fournisseurs de services. S'il s'avère impossible d'obtenir un tel consentement, la communication de ces données à des tiers devrait être réglementée. Toutefois, en dehors d'une réglementation dans ce domaine, d'autres possibilités s'offrent au législateur et notamment des possibilités techniques. On a vu qu'en France, le système kiosque permet un accès anonyme de l'individu aux données. Seul le temps de consultation du service par l'individu est comptabilisé, l'anonymat des informations consultées est respecté. Cela résout donc un certain nombre des problèmes évoqués ci-dessus. La seule question en suspens dans ce cas est celle de la sécurité de la transmission, problème qui sera abordé plus tard.

Si le principe de finalité défini par la Convention reste plus que jamais valable dans le contexte des nouvelles technologies, il semble nécessaire de l’assortir de garanties supplémentaires en ce qui concerne les médias interactifs, vu l'impossibilité de procéder à un véritable contrôle du respect de la finalité étant donné le nombre de données collectées et la multiplication des services offerts par les médias interactifs.

6. Article 5.d - Le principe d'exactitude

Il est important de s'assurer que les données transportées dans un système vidéotex ou de courrier électronique ne soient pas déformées. La transmission, par exemple, de données médicales inexactes peut avoir de graves conséquences, des mesures devraient donc être prises pour assurer une bonne qualité de transmission. Le problème de l'exactitude se pose également au niveau de la collecte. Dans tous les cas, il paraît important que l'individu puisse avoir un droit de regard sur les données collectées à son sujet.

On peut également s'interroger sur l'exactitude des profils établis à partir des informations collectées lors de la consultation d'un service par un individu. Pour traiter ce problème, il convient de se référer à la question de la finalité de la collecte dans le domaine des médias interactifs. On a vu que le fournisseur de services pouvait avoir un intérêt légitime à utiliser de telles données pour ses besoins propres (à des fins de gestion ou de politique de vente). On pourrait également imaginer que le fournisseur de services établisse des profils de l'individu dans un tel but. En aucun cas, l'établissement de tels profils ne devrait permettre de porter un jugement sur une personne. La transmission de telles informations devrait également s'accompagner de

garanties appropriées: consentement libre et éclairé de la personne concernée où, si cela s'avère impossible, autorisation légale.

La réalisation d'un sondage d'opinion par le biais du vidéotex devrait s'accompagner de garanties supplémentaires. Il convient de veiller à ce que de telles informations ne soient pas divulguées. Une fois le sondage réalisé, les données devraient être effacées et le secret des choix faits par les personnes respecté.

Dans la mesure où le principe de finalité pour la collecte et l'utilisation des données est respecté et où la transmission à des tiers de telles données est soigneusement réglementée, l'établissement de profils sur des individus ne peut véritablement représenter un danger pour ces derniers. Les profils ne constituent en effet qu'une vue parcellaire de ces individus pour le fournisseur de services. La transmission systématique de telles données à d'autres fournisseurs pourrait par contre représenter un danger pour l'individu concerné.

7. Article 7 - Sécurité des données

La sécurité des données constitue un problème clé qui se pose pour les trois technologies étudiées, que ce soit le vidéotex interactif, le courrier électronique ou la surveillance à distance d'une maison individuelle. Même si la collecte, l'utilisation ou la transmission de données à caractère personnel sont entourées de toutes les garanties nécessaires, ces dernières sont inutiles si quelqu'un peut pénétrer sur le réseau et avoir accès à de telles données. Il s'agit là d'un problème crucial dont les utilisateurs n'ont pas toujours conscience.

Différentes techniques permettent à l'heure actuelle la protection physique des centres de traitement: protection contre les pannes électriques, protection contre le feu, contrôle de l'accès ou des intrusions. Au niveau des trois technologies étudiées, c'est principalement ce dernier aspect que nous retiendrons. Le contrôle de l'accès ou des intrusions, qui vise à restreindre l'accès à des traitements de données ou à des transactions, peut être fait par le biais de l'identification du correspondant ou de l'utilisateur qui peut être effectuée à quatre niveaux: identification de la ligne reliant le terminal à l'ordinateur, identification du terminal, identification de l'abonné ou de l'opérateur (ce dernier pouvant être autorisé par l'abonné à utiliser le terminal). Les contrôles consistent généralement en la vérification d'un code, d'un mot de passe, d'une réponse à une question personnelle ou du contenu d'une carte magnétique - méthodes les plus couramment utilisées à l'heure actuelle - et sont effectués par un système central, par exemple par le service auquel on demande l'accès. Une étude réalisée par la Communauté économique européenne sur les techniques de sécurité et de protection des données montre que de tels contrôles ne sont pas aussi fiables que les contrôles effectués aux niveaux locaux, c'est-à-dire par le biais du terminal lui-même et non par l'ordinateur central; en effet, dans ce dernier cas, la personne qui demande l'accès est déjà en communication avec le système au cours de la procédure d'identification; cette dernière peut être imparfaite et permettre alors à un utilisateur mal intentionné d'avoir accès au service demandé.

L'identification peut également être nécessaire pour des besoins de preuve dès lors qu'une transaction est effectuée. En raison de l'imperfection des méthodes d'identification énumérées ci-dessus, d'autres méthodes ont été développées ou sont en

cours de développement: vérification de la signature, reconnaissance de là voix, reconnaissance des empruntes digitales et autres méthodes telles que la reconnaissance de l'empreinte de la paume, de la rétine, etc. On peut également citer la carte à mémoire qui va sans doute connaître d'importants développements à l'avenir car elle constitue un moyen d'identification sûr et confidentiel.

Dans le domaine du vidéotex et du courrier électronique, il convient également de protéger les données qui sont transmises sur les lignes de communication ou qui sont enregistrées sur des supports informatiques. Parmi les techniques de sécurité, on peut citer: le codage des informations, les méthodes de chiffrement, les systèmes cryptographiques.

Pour les systèmes de courrier électronique, il paraît également important d'avoir la possibilité de garder trace de toute transaction effectuée sur le réseau: identification de l'expéditeur, identification du destinataire, numéro du message, date et heure d'arrivée, nombre de pages, etc.

On peut conclure que, si le problème de la sécurité informatique n'est pas nouveau et faisait déjà l'objet des préoccupations des rédacteurs de la Convention, il est indéniable qu'il à pris une importance primordiale au fur et à mesure du développement de la technologie et de la pénétration de l'informatique dans les foyers.

8. Article 8 - Les droits de la personne concernée et article 10 - Recours

Les lois sur la protection des données prévoient la déclaration ou l'autorisation de tout traitement de données à caractère personnel ainsi' que l'exercice des droits d'accès ou de rectification vis-à-vis de ces traitements. On a vu toutefois que l'exercice de ces droits ne pouvait s'effectuer tel quel en ce qui concerne le courrier électronique, domaine dans lequel il s'agit de respecter le secret de la correspondance. Dans ce même domaine du courrier électronique, il faudrait également prévoir un droit de recours pour l'individu, en cas, par exemple, d'erreur dans la transmission des messages. On a vu qu'à l'heure actuelle, notamment dans le secteur public, le transporteur n'est pas responsable, excepté en cas de fautes lourdes. Toutefois, ce problème d'erreur de transmission peut être résolu au niveau de la sécurité: il existe en effet des mesures techniques visant à éviter ce genre d'erreurs, notamment par le biais de la double transmission, ou la correction automatique des erreurs.

Grâce au vidéotex, il est désormais possible d'accéder à des journaux sur support électronique. Il devient donc nécessaire de prévoir une extension éventuelle des lois sur la presse (diffamation, droit de réponse) à ces nouveaux types de journaux, ou alors il faudrait envisager des règles additionnelles ou des recours pour les individus. Un droit de réponse est prévu par la nouvelle loi française sur la liberté de communication.

9 Article 12 - Flux transfrontières de données

Si, comme il est dit au début de ce chapitre, le volume des données à caractère personnel en circulation s'est accru de façon dramatique, il est certain que la circulation transfrontière de telles données s'est également développée et continuera à le faire. Les tendances technologiques décrites au chapitre 2 rendent ces conclusions

inévitables. En conséquence, on peut s'attendre à ce que les modèles de circulation de l'information utilisés dans le rapport afin de distinguer les différentes technologies auront de plus en plus un caractère transnational. Le vidéotex, par exemple, permet désormais à ses utilisateurs d'avoir accès à des bases de données situées dans différents pays. Les transporteurs internationaux utilisant les satellites et les fibres optiques ont contribué de façon considérable à la promotion de l'utilisation du courrier électronique et des autres technologies correspondant au modèle conversationnel. Toutefois, au fur et à mesure que le volume des flux transfrontières se développe, les possibilités de contrôle diminuent, Il devient beaucoup plus difficile, par exemple, d'identifier les pays à travers lesquels les données transiteront avant d'atteindre le destinataire autorisé. Les problèmes de sécurité et de confidentialité des données sont accrus lorsque ces données passent à travers des lignes téléphoniques qui traversent des pays où l'on accorde peu ou pas d'attention au problème de protection des données. Le problème de la communication transfrontière de données sensibles se pose avec acuité.

En résumé, lorsque des réseaux de communication permettent à des hommes d'affaires en voyage à l'étranger d'avoir accès aux bases de données de leurs entreprises, par le biais d'ordinateurs portables pouvant se brancher dans des aéroports, et de mettre instantanément à leur disposition dans leur ordinateur ces données à travers de grandes distances, la question des réglementations nationales en matière de flux transfrontières de données devient véritablement problématique.

Le caractère transnational du traitement des données pose inévitablement des problèmes de compétence en ce qui concerne la loi applicable. La Convention est muette sur ce problème particulier. Toutefois, il paraît souhaitable de parvenir à des «règles d'arbitrages» afin de résoudre les différends dans le domaine des flux transfrontières. Il se peut qu'un fichier de données soit enregistré dans un pays A, que le «maître du fichier» réside dans un pays B et que la personne concernée soit domiciliée dans un pays C. Quelle loi dans ce cas devrait être appliquée si, en raison d'un accès non autorisé au fichier, il est porté atteinte à la personne concernée dans un pays D?

L'accès d'un utilisateur à un système de données situé à l'étranger peut également poser des problèmes en ce qui concerne l'application extra-territoriale de la loi sur la protection des données du pays de l'utilisateur. Est-ce que le fait que le terminal autorisant l'accès soit situé dans un pays X implique que les opérations de traitement de ces données effectuées par le «maître du fichier» dans un pays Y tombent sous le contrôle du pays X? Ou alors doit-on appliquer la loi du pays où le système de traitement des données est situé?

7. Conclusion

Il convient tout d'abord de préciser que les principes de la Convention ont un caractère général. Comme les garanties constitutionnelles ou internationales en matière de droits de l'homme, les principes pour la protection des données sont énoncés en des termes permettant une adaptation aux situations en évolution. Pour la résolution des problèmes posés par les nouvelles technologies, il est proposé de prendre pour point de départ les principes généraux, quel que soit le problème abordé' droit d'accès, qualité des données, flux transfrontières de données' Rappelons que la protection des

données constitue un droit fondamental de l'homme, intimement lié au droit au respect de la vie privée. Le droit au respect de la vie privée lui-même, tel que garanti par exemple par l'article 8 de la Convention européenne des Droits de l'Homme, se révèle particulièrement efficace face aux menaces technologiques. La Cour et la Commission européennes des Droits de l'Homme ont toutes deux montré leur volonté d'appliquer ce droit à des problèmes tels que les écoutes téléphoniques les mises en relation de fichiers, les accès non autorisés aux données à caractère personnel - problèmes qui n'étaient probablement pas venus à l'esprit des rédacteurs de la Convention européenne des Droits de l'Homme.

Des problèmes spécifiques peuvent, en outre, faire l'objet de solutions spécifiques basées sur les principes généraux de la protection des données. C'est là l'intérêt de l'approche sectorielle aux problèmes e protection des données, activement encouragée par le Conseil de l'Europe depuis l'ouverture à la signature de la Convention. Les recommandations adoptées jusqu'à présent par le Comité des Ministres, par exemple, dans les domaines de la recherche scientifique et des statistiques (n° R (83) 10), de la sécurité sociale (n° R (86) 1) constituent des tentatives d'interprétation des principes de la Convention dans des contextes particuliers de traitement des données. Il n'y a pas de raison de ne pas trouver d'autres solutions, basées sur les principes généraux de la Convention, aux problèmes posés par les nouvelles technologies. Les analyses sur la télémétrie, les médias interactifs et les systèmes de courrier électronique montrent qu'il est tout à fait possible de trouver un cadre réglementaire spécifique, une fois les problèmes correctement identifiés. En l'absence de réglementation spécifique ou d'autoréglementation, on peut considérer qu'une approche «éclairée», basée sur les principes généraux, des problèmes de protection des données découlant des nouvelles technologies, de la part des personnes responsables de l'application des normes sur la protection des données, peut diminuer de façon considérable les possibilités d'atteintes à la vie privée.

Comme il a été dit précédemment, les cours constitutionnelles, aux niveaux national et international, ont montré qu'elles pouvaient interpréter les droits fondamentaux de l'homme de manière à les adapter aux nouveaux changements de la société. Il se peut également que le comité Consultatif constitué Conformément à la Convention pour la protection des données trouve des solutions pour interpréter les principes de la Convention de manière que ces derniers continuent à être adaptés à notre ère technologique.