Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

Préface

Compte tenu de l'essor pris par le traitement automatique de l'information, qui permet de transmettre de vastes quantités de données en quelques secondes à travers les frontières nationales et même à travers les continents, il a fallu étudier la question de la protection de la vie privée sous l'angle des données de caractère personnel. Des législations relatives à la protection de la vie privée ont été adoptées ou le seront prochainement dans près de la moitié des pays de l'OCDE (l'Allemagne, l'Autriche, le Canada, le Danemark, les Etats-Unis, la France, le Luxembourg, la Norvège et la Suède ont promulgué une législation. La Belgique, l'Espagne, les Pays-Bas et la Suisse ont établi des projets de loi) en vue de prévenir des actes considérés comme constituant des violations des droits fondamentaux de l'homme, tels que le stockage illicite de données de caractère personnel qui sont inexactes, l'utilisation abusive ou la divulgation non autorisée de ces données.

En revanche, il est à craindre que des disparités dans les législations nationales n'entravent la libre circulation des données de caractère personnel à travers les frontières; or, cette circulation s'est considérablement intensifiée au cours des dernières années et elle est appelée à se développer encore par suite de l'introduction généralisée de nouvelles technologies des ordinateurs et des télécommunications. Des restrictions imposées à ces flux pourraient entraîner de graves perturbations dans d'importants secteurs de l'économie, tels que la banque et les assurances.

C'est pourquoi, les pays Membres de l'OCDE ont jugé nécessaire d'élaborer des lignes directrices qui permettraient d'harmoniser les législations nationales relatives à la protection de la vie privée et qui, tout en contribuant au maintien de ces droits de l'homme, empêcheraient que les flux internationaux de données ne subissent des interruptions. Ces lignes directrices sont l'expression d'un consensus sur des principes fondamentaux qui peuvent être intégrés à la législation nationale en vigueur ou servir de base à une législation dans les pays qui ne sont pas encore dotés.

Les lignes directrices, qui revêtent la forme d'une recommandation du conseil de l'OCDE, ont été élaborées par un groupe d'experts gouvernementaux placé sous la présidence de M. M.D. Kirby, Président de la Commission australienne de la réforme législative. Cette recommandation a été adoptée et a pris effet le 23 septembre 1980.

Les lignes directrices sont accompagnées d'un exposé des motifs destiné à fournir des éléments d'information sur les débats et les raisonnements qui sous-tendent leur énoncé.

RECOMMANDATION DU CONSEIL CONCERNANT LES LIGNES DIRECTRICES REGISSANT LA PROTECTION DE LA VIE PRIVEE ET LES FLUX TRANSFRONTIERES DE DONNEES DE CARACTERE PERSONNEL (23 septembre 1980)

LE CONSEIL

Vu les Articles 1 (c), 3 (a) et 5 (b) de la Convention relative à l'Organisation de Coopération et de Développement Economiques en date du 14 décembre 1960;

RECONNAISSANT :

- que, bien que les législations et politiques nationales puissent différer, il est de l'intérêt commun des pays Membres de protéger la vie privée et les libertés individuelles et de concilier des valeurs à la fois fondamentales et antagonistes, telles que le respect de la vie privée et la libre circulation de l'information;
- que le traitement automatique et les flux transfrontières de données de caractère personnel créent de nouvelles formes de relations entre pays et exigent l'instauration de règles et pratiques compatibles;
- que les flux transfrontières de données de caractère personnel contribuent au développement économique et social;
- que les droits internes concernant la protection de la vie privée et les flux transfrontières de données de caractère personnel sont susceptibles d'entraver ces flux transfrontières.

Résolu à favoriser la libre circulation de l'information entre les pays Membres et à éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre ces pays;

RECOMMANDE

- Que les pays Membres tiennent compte, dans leur législation interne, des principes concernant la protection de la vie privée et des libertés individuelles exposés dans les lignes directrices figurant en Annexe à la présente Recommandation dont elle fait partie intégrante;
- Que les pays Membres s'efforcent de supprimer ou d'éviter de créer, au nom de la protection de la vie privée, des obstacles injustifiés aux flux transfrontières des données de caractère personnel;
- Que les pays Membres coopèrent pour mettre en oeuvre les lignes directrices énoncées en Annexe;
- Que les pays Membres conviennent dès que possible de procédures spécifiques de consultation et de coopération en vue de l'application des présentes lignes directrices.

Annexe à la Recommandation du Conseil du 23 Septembre 1980: LIGNES DIRECTRICES REGISSANT LA PROTECTION DE LA VIE PRIVEE ET LES FLUX TRANSFRONTIERES DE DONNEES DE CARACTERE PERSONNEL

PREMIERE PARTIE. CONSIDERATIONS GENERALES DEFINITIONS

1. Aux fins des présentes lignes directrices:

a) par « maître du fichier », on entend toute personne physique ou morale qui, conformément au droit interne, est habilitée à décider du choix et de l'utilisation des données de caractère personnel, que ces données soient ou non collectées, enregistrées, traitées ou diffusées par ladite personne ou par un agent agissant en son nom;

b) par « données de caractère personnel », on entend toute information relative à une personne physique identifiée ou identifiable (personne concernée);

c) par « flux transfrontière de données de caractère personnel », on entend la circulation de

données de caractère personnel à travers les frontières nationales.

Champ d'application des lignes directrices

2. Les présentes lignes directrices s'appliquent aux données de caractère personnel, dans les secteurs public et privé, qui, compte tenu de leur mode de traitement, de leur nature ou du contexte dans lequel elles sont utilisées, comportent un danger pour la vie privée et les libertés individuelles.

3. Les présentes lignes directrices ne devraient pas être interprétées comme interdisant:

a) d'appliquer, à diverses catégories de données de caractère personnel, des mesures de protection différentes selon leur nature et le contexte dans lequel elles sont collectées, enregistrées, traitées ou diffusées;

b) d'en exclure l'application à des données de caractère personnel qui, manifestement, ne présentent aucun risque pour la vie privée et les libertés individuelles, ou

c) d'en limiter l'application au traitement automatique des données de caractère personnel.

4. Les exceptions aux principes énoncés dans les Parties Deux et Trois des présentes lignes directrices, y compris celles intéressant la souveraineté nationale, la sécurité nationale et l'ordre public, devraient être:

a) aussi peu nombreuses que possible, et

b) portées à la connaissance du public.

5. Dans le cas particulier des pays à structure fédérale, l'application des présentes lignes directrices peut être influencée par la répartition des pouvoirs dans l'Etat fédéral.

6. Les présentes lignes directrices devraient être considérées comme des normes minimales susceptibles d'être complétées par d'autres mesures visant à protéger la vie privée et les libertés individuelles.

PARTIE DEUX. PRINCIPES FONDAMENTAUX APPLICABLES AU PLAN NATIONAL

Principe de la limitation en matière de collecte

7. Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Principe de la qualité des données

8. Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

Principe de la spécification des finalités

9. Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

Principe de la limitation de l'utilisation

10. Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe 9, si ce n'est:

a) avec le consentement de la personne concernée; ou

b) lorsqu'une règle de droit le permet.

Principe des garanties de sécurité

11. Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, ou divulgation non autorisés.
Principe de la transparence

12. Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

Principe de la participation individuelle

13. Toute personne physique devrait avoir le droit:

a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;

b) de se faire communiquer les données la concernant;

i) dans un délai raisonnable;

ii) moyennant, éventuellement, une redevance modérée;

iii) selon des modalités raisonnables; et

iv) sous une forme qui lui soit aisément intelligible;

c) d'être informée des raisons pour lesquelles une demande quelle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet; et

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Principe de la responsabilité

14. Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

PARTIE TROIS. PRINCIPES FONDAMENTAUX APPLICABLES AU PLAN INTERNATIONAL: LIBRE CIRCULATION ET RESTRICTIONS LEGITIMES

15. Les pays Membres devraient prendre en considération les conséquences pour d'autres pays Membres d'un traitement effectué sur leur propre territoire et de la réexportation des données de caractère personnel.

16. Les pays Membres devraient prendre toutes les mesures raisonnables et appropriées pour assurer que les flux transfrontières de données de caractère personnel, et notamment le transit par un pays Membre, aient lieu sans interruption et en toute sécurité.

17. Un pays Membre devrait s'abstenir de limiter les flux transfrontières de données de caractère personnel entre son territoire et celui d'un autre pays Membre, sauf lorsqu'un ce dernier ne se conforme pas encore pour l'essentiel aux présentes Lignes directrices ou lorsque la réexportation desdites données permettrait de contourner sa législation interne sur la protection de la vie privée et des libertés individuelles. Un pays Membre peut également imposer des restrictions à l'égard de certaines catégories de données de caractère personnel pour lesquelles sa législation interne sur la protection de la vie privée et les libertés individuelles prévoit des réglementations spécifiques en raison de la nature de ces données et pour lesquelles l'autre pays Membre ne prévoit pas de protection équivalente.

18. Les pays Membres devraient éviter d'élaborer des lois, des politiques et des procédures, qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel qui iraient au-

delà des exigences propres à cette protection.

PARTIE QUATRE. MISE EN OEUVRE DES PRINCIPES A L'ECHELON NATIONAL

19. Lors de la mise en oeuvre, au plan intérieur, des principes énoncés dans les Parties Deux et Trois, les pays Membres devraient établir des procédures juridiques, administratives et autres, ou des institutions pour protéger la vie privée et les libertés individuelles eu égard aux données de caractère personnel. Les pays Membres devraient notamment s'efforcer de:

a) adopter une législation nationale appropriée;

b) favoriser et soutenir des systèmes d'auto-réglementation (codes de déontologie ou autres formes);

c) permettre aux personnes physiques de disposer de moyens raisonnables pour exercer leurs droits;

d) instituer des sanctions et des recours appropriés en cas d'inobservation des mesures mettant en oeuvre les principes énoncés dans les Parties Deux et Trois, et

e) veiller à ce que les personnes concernées ne fassent l'objet d'aucune discrimination inéquitable.

PARTIE CINQ. COOPERATION INTERNATIONALE

20. Les pays Membres devraient, sur demande, faire connaître à d'autres pays Membres les modalités détaillées de l'application des principes énoncés dans les présentes lignes directrices. Les pays Membres devraient également veiller à ce que les procédures applicables aux flux transfrontières de données de caractère personnel, ainsi qu'à la protection de la vie privée des libertés individuelles, soient simples et compatibles avec celles des autres pays Membres qui se confirment aux présentes lignes directrices.

21. Les pays Membres devraient établir des procédures en vue de faciliter:

l'échange d'informations relatives aux présentes lignes directrices; et l'assistance mutuelle lorsqu'il s'agit des questions de procédure et d'échange réciproque d'information.

22. Les pays Membres devraient s'employer à établir des principes, au plan intérieur et international, afin de déterminer le droit applicable en cas de flux transfrontières de données de caractère personnel.

EXPOSE DES MOTIFS

INTRODUCTION

La dernière décennie a été marquée, dans les pays Membres de l'OCDE, par l'apparition de lois visant à protéger la vie privée. Ces lois ont eu tendance à revêtir des formes différentes selon les pays et elles sont encore en cours d'élaboration dans un grand nombre d'entre eux. Les disparités dans les législations peuvent susciter des obstacles à la libre circulation de l'information entre pays. Cette circulation s'est fortement intensifiée au cours des dernières années et cette tendance ne peut que s'amplifier par suite de l'introduction de nouvelles technologies de l'informatique et des communications.

L'OCDE, qui a mené des travaux dans ce domaine depuis quelques années, a décidé de se pencher sur les problèmes que soulèvent des législations nationales. Ce groupe a maintenant achevé ses travaux.

Les lignes directrices revêtent un caractère général et reflètent les délibérations et les travaux législatifs qui ont été menés pendant plusieurs années dans les pays Membres. Le Groupe d'experts, qui a établi les lignes directrices, a estimé essentiel de les accompagner

d'un Exposé des motifs dans le but d'expliquer et de préciser les lignes directrices et les problèmes fondamentaux que soulève la protection de la vie privée et des libertés individuelles. L'Exposé attire l'attention sur les questions clés qui se sont dégagées des échanges de vues relatifs aux lignes directrices et énonce les raisons du choix de certaines solutions particulières.

La première partie de l'Exposé présente des considérations d'ordre général concernant le domaine étudié, tel qu'il est perçu dans les pays Membres. Elle explique la nécessité d'une action internationale et récapitule les travaux menés jusqu'alors par l'OCDE et certaines autres organisations internationales. En conclusion, elle recense les principaux problèmes rencontrés par le Groupe d'experts dans l'accomplissement de sa tâche.

La Partie Deux comporte deux subdivisions : la première est consacrée à des commentaires concernant certaines caractéristiques générales des lignes directrices, alors que la seconde contient des observations détaillées sur divers paragraphes.

Le présent Exposé des motifs est un document d'information établi en vue d'expliquer et de décrire d'une façon générale les travaux du Groupe d'experts. Il est subordonné aux lignes directrices elles-mêmes, dont il ne peut modifier la teneur, mais il est fourni afin d'en aider l'interprétation et l'application.

I. CONSIDERATIONS D'ORDRE GENERAL

Les problèmes

1. On peut dire que les années 70 ont été marquées par une intensification des travaux de recherche et des activités législatives concernant la protection de la vie privée eu égard à la collecte et à l'utilisation des données de caractère personnel. Il ressort de nombreux rapports officiels que les problèmes sont considérés avec sérieux au niveau politique, mais qu'en revanche il est difficile de concilier des intérêts antagonistes et peu probable que l'on y parvienne de façon définitive. L'opinion publique a été encline à s'axer sur les risques et incidence que comporte le traitement automatisé des données de caractère personnel et certains pays ont décidé de promulguer des textes de loi qui traitent exclusivement de l'informatique et des activités fondées sur l'informatique. D'autres pays ont préféré aborder les questions de protection de la vie privée d'un point de vue plus général sans tenir compte de la technologie particulière de traitement de l'information en cause.

2. Les mesures correctives actuellement à l'étude comprennent principalement des garanties offertes à l'individu en vue d'empêcher une intrusion dans sa vie privée au sens classique du terme, c'est-à-dire l'utilisation abusive ou la divulgation de données concernant l'intimité des personnes; cependant, la nécessité d'assurer une protection s'est manifestée dans d'autres domaines plus ou moins proches. L'obligation pour les maîtres de fichier d'informer le grand public des activités de traitement des données et le droit des personnes concernées de faire compléter ou amender les données existant à leur sujet sont deux exemples pris au hasard. Dans l'ensemble, on a eu tendance à élargir le concept traditionnel de la vie privée (soit le « droit d'avoir la paix ») en établissant une synthèse plus complexe des différents intérêts en jeu que le terme de vie privée et libertés individuelles permet probablement de définir de façon plus correcte.

3. En ce qui concerne les problèmes juridiques soulevés par le traitement automatique de l'information, la protection de la vie privée et des libertés individuelles constitue peut être l'aspect qui suscite les plus larges controverses. Cette préoccupation très répandue s'explique notamment du fait que les ordinateurs sont partout utilisés pour le traitement des données de caractère personnel, que les possibilités d'enregistrement, de comparaison, de rapprochement et de choix des données de caractère personnel, ainsi que d'accès à ces dernières, se sont considérablement élargies et que la fusion de la technologie des ordinateurs et de celle des télécommunications risque de mettre les données de caractère

personnel simultanément à la disposition de milliers d'utilisateurs géographiquement dispersés, de même qu'elle permet la mise en commun des données et la création de réseaux de données complexes à l'échelon national et international. Il s'avère particulièrement urgent d'étudier certains problèmes, notamment ceux que posent les nouveaux réseaux internationaux de données et la nécessité de concilier les intérêts antagonistes liés, d'une part, à la protection de la vie privée et, de l'autre, à la liberté de l'information, afin de pouvoir pleinement exploiter les possibilités des technologies modernes du traitement de l'information, dans la mesure où cela est souhaitable.

Activités à l'échelon national

4. A ce jour, plus d'un tiers des pays Membres de l'OCDE ont promulgué une ou plusieurs lois qui, notamment, visent à protéger les personnes physiques contre l'utilisation abusive de données les concernant et à leur conférer le droit d'accès à ces données en vue d'en vérifier l'exactitude et l'adéquation. Dans les Etats à structure fédérale, des législations de ce type peuvent exister tant au niveau national qu'à celui des Etats ou des provinces. La dénomination donnée à ces lois varie selon les pays. Ainsi il est de pratique courante, en Europe continentale, de parler de « lois sur les données » ("data laws") ou de « loi sur la protection des données », alors que dans les pays anglophones, elles sont habituellement qualifiées de "privacy protection laws" (lois sur la protection de la vie privée). Ces textes de loi ont, pour la plupart, été promulgués après 1973 et la période actuelle peut être considérée comme se caractérisant par la poursuite, voire l'élargissement, de l'activité législative. Les pays dans lesquels des textes de loi sont déjà en vigueur, se tournent vers de nouveaux domaines susceptibles de faire l'objet d'une protection ou s'emploient à réviser ou à compléter les textes existants. Plusieurs autres pays qui accèdent à ce domaine ont des projets de loi en attente ou étudient les problèmes en vue d'élaborer une législation. Ces efforts au plan national et en particulier, les importants rapports et documents de recherche établis par des commissions publiques ou des organismes analogues contribuent à élucider les problèmes, de même qu'à montrer les avantages et les conséquences de diverses solutions. Au stade actuel, ils offrent un fondement solide à l'action internationale.

5. Les démarches adoptées par les divers pays à l'égard de la protection de la vie privée et des libertés individuelles ont de nombreux traits communs. Il est donc possible de définir certains intérêts ou valeurs de base qui sont couramment considérés comme étant les composants élémentaires du domaine de la protection. Parmi les principes fondamentaux de ce type figurent les suivants : assigner des limites à la collecte des données de caractère personnel suivant les objectifs de la personne chargée de cette collecte et des critères analogues, limiter l'utilisation des données de manière à se conformer à des finalités déclarées, créer les moyen permettant aux personnes physiques de connaître l'existence et le contenu des données et de les faire corriger, déterminer les personnes physiques ou morales qui sont chargées de faire observer les règles et décisions ayant trait à la protection de la vie privée. En termes généraux, les textes de loi destinés à assurer la protection de la vie privée et les libertés individuelles en liaison avec les données de caractère personnel visent à couvrir les étapes successives du cycle qui commence par la collecte initiale des données pour s'achever avec leur effacement ou des mesures analogues, et à garantir dans toute la mesure du possible que les intéressés auront connaissance de ce processus, pourront y participer et le contrôler.

6. Les différences entre les démarches nationales, telles qu'elles se dégagent à l'heure actuelle des lois, projets de lois ou propositions de législation, concernent des aspects tels que la portée de la législation, l'importance accordée à divers éléments de la protection, les modalités détaillées de mise en oeuvre des principes généraux susmentionnés et le mécanisme d'application. Il apparaît donc que les opinions divergent quant aux prescriptions en matière d'autorisation et aux mécanismes de contrôle revêtant la forme d'organes de

tutelle spéciaux « autorités chargées de l'inspection des données ». On constate que les catégories de données sensibles sont définies de façon différente et que les moyens employés pour assurer la transparence et la participation individuelle varient, pour ne citer que quelques exemples. Il va de soi que les différences traditionnelles existant entre les régimes juridiques entraînent des disparités, aussi bien dans les façons de légiférer que dans l'élaboration détaillée du cadre réglementaire applicable à la protection des données de caractère personnel.

Aspects internationaux de la protection des données individuelles et des banques de données

7. Pour un certain nombre de raisons, les problèmes que pose la mise au point de garanties individuelles en liaison avec le traitement des données de caractère personnel ne peuvent être résolus exclusivement au niveau national. L'accroissement considérable des flux de données à travers les frontières nationales et la création de banques internationales de données (collections de données destinées à être extraites et à d'autres fins) ont mis en évidence la nécessité d'une action nationale concertée, tout en venant étayer les arguments en faveur de la libre circulation de l'information, qui doit souvent être considérée en regard des exigences liées à la protection des données et des limitations imposées à la collecte, au traitement et à la diffusion de ces données.

8. A l'échelon international, on se préoccupe avant tout de parvenir à un consensus au sujet des principes fondamentaux sur lesquels doit reposer la protection des personnes physiques. Un tel consensus supprimerait ou diminuerait les raisons de réglementer l'exportation des données et faciliterait la solution des problèmes soulevés par les conflits de loi. En outre, il pourrait marquer un premier pas sur la voie de l'élaboration d'accords internationaux plus détaillés ayant force exécutoire.

9. Il y a d'autres raisons pour lesquelles la réglementation du traitement des données de caractère personnel devrait être envisagée dans un contexte international : les principes en jeu concernent des valeurs que de nombreux pays sont très soucieux de sauvegarder et de voir généralement acceptées; ils peuvent aider à réaliser des économies sur les coûts afférents à la circulation internationale de l'information, il est de l'intérêt commun des pays d'empêcher la constitution d'enclaves dans lesquelles on pourrait facilement se soustraire aux règlements nationaux en matière de traitement de l'information; en fait, compte tenu de la mobilité internationale des individus, des biens et des activités commerciales et scientifiques, des pratiques acceptées d'un commun accord eu égard au traitement des données peuvent comporter des avantages, même lorsque la circulation de l'information à travers les frontières n'est pas directement en cause.

Activités internationales y afférentes

10. Il existe plusieurs accords internationaux sur divers aspects des télécommunications qui, tout en facilitant les relations et la coopération entre les peuples, reconnaissent pleinement à chaque pays le droit souverain de réglementer ses télécommunications (Convention internationale des télécommunications de 1973). La protection des données informatisées et des programmes de calcul a été étudiée notamment par l'Organisation Mondiale de la Propriété Intellectuelle, qui a mis au point un projet de dispositions types pour des législations nationales applicables à la protection du logiciel. On peut trouver des accords spécialisés visant à instaurer une coopération informationnelle dans un certain nombre de domaines, tels que l'application de la loi, les services de santé, les statistiques et les services judiciaires (notamment en ce qui concerne le recueil de témoignages).

11. Un certain nombre d'accords internationaux traitent de façon plus générale des questions qui sont actuellement à l'étude, à savoir la protection de la vie privée et la libre

diffusion de l'information. Il s'agit notamment de la Convention européenne des droits de l'homme en date du 4 novembre 1950 et du Pacte international relatif aux droits civiques et politiques (Nations Unies, 19 décembre 1966).

12. Cependant, compte tenu de l'insuffisance des instruments internationaux en vigueur eu égard au traitement de l'information et aux droits de la personne, plusieurs organisations internationales ont procédé à une étude détaillée des problèmes en cause afin d'aboutir à des solutions plus satisfaisantes.

13. En 1973 et 1974, le Comité des Ministres du Conseil de l'Europe a adopté deux résolutions relatives à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques respectivement dans le secteur prive et dans le secteur public. Dans ces deux résolutions, il est recommandé aux gouvernements des Etats membres du Conseil de l'Europe de prendre les mesures nécessaires pour appliquer un certain nombre de principes fondamentaux de protection concernant l'obtention de données, la qualité des données et le droit des personnes physiques d'être informées de l'existence des données et des activités de traitement de l'information.

14. Par la suite, le Conseil de l'Europe a, conformément aux instructions de son Comité des Ministres, commencé à établir une Convention internationale sur la protection de la vie privée par rapport au traitement des données à l'étranger et au traitement transfrontière des données. Il a aussi entrepris des travaux sur des modèles de règlements applicables aux banques de données médicales et de codes de conduite destinés aux informaticiens. La Convention a été adoptée par le Comité des Ministres le 17 septembre 1980. Elle vise à établir des principes fondamentaux pour la protection des données qui seront appliquées par les pays Membres, à réduire les limitations imposées aux flux transfrontières de données entre les Parties contractantes sur une base de réciprocité, à instaurer une coopération entre les autorités nationales chargées de la protection des données, de même qu'à créer un comité consultatif pour l'application et la mise au point suivie de la Convention.

15. La Communauté Européenne a effectué des études sur les problèmes de l'harmonisation des législations nationales au sein de la Communauté en liaison avec les flux transfrontières de données et d'éventuelles distorsions de la concurrence, les problèmes relatifs à la sécurité et au caractère confidentiel des données et la nature des flux transfrontières de données. Une sous-commission du Parlement Européen a organisé, au début de 1978, un débat public sur l'informatique et les droits de la personne. Ses travaux ont débouché sur la présentation d'un rapport au Parlement Européen au printemps de 1979. Ce rapport, qui a été adoptés par le Parlement Européen en mai 1979, contient une résolution sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique.

Activités de l'OCDE

16. Le programme de l'OCDE relatif aux flux transfrontières de données s'inspire des études sur l'informatique dans le secteur public qui ont été entreprises en 1969. Un Groupe d'experts, à savoir le Sous-groupe sur les banques de données, a analysé et étudié différents aspects de la question de la protection des libertés individuelles, notamment en liaison avec l'information numérique, l'administration publique, les flux transfrontières de données et les incidences au plan de l'action gouvernementale en général. Afin de rassembler des éléments de faits sur la nature des problèmes, le Sous-groupe sur les banques de données a organisé en 1977 à Vienne un Colloque, qui a permis d'obtenir des avis et des données d'expériences émanant de divers milieux intéressés, notamment de l'administration publique, de l'industrie, des utilisateurs de réseaux internationaux de transmission de données, de services de traitement de l'information et d'organisations internationales concernées.

17. Un certain nombre de principes directeurs ont été élaborés dans un contexte de manière à pouvoir donner lieu à une action internationale. Ces principes admettaient :

- (a) la nécessité d'une circulation généralement permanente et sans faille de l'information entre pays;
- (b) l'intérêt légitime des pays à empêcher les transferts de données qui sont dangereux pour leur sécurité ou contraires à leurs lois sur l'ordre public et les bonnes moeurs ou qui violent les droits de leurs citoyens;
- (c) la valeur économique de l'information et l'importance qu'il y a à protéger les « échanges de données » grâce à des règles admises de concurrence non déloyale,
- (d) la nécessité de prévoir des garanties de sécurité afin de réduire au minimum les violations de données possédées en propre et l'utilisation abusive des données de caractère personnel et
- (e) la portée qu'aurait une adhésion des pays à un recueil de principes fondamentaux applicables à la protection des données de caractère personnel.

18. Au début de 1978, un nouveau Groupe ad hoc d'experts sur les obstacles au mouvement transfrontière des données et la protection des libertés individuelles a été créé dans le cadre de l'OCDE; il a été chargé d'élaborer des lignes directrices relatives aux règles fondamentales régissant le mouvement transfrontière des données de caractère personnel et la protection des libertés individuelles, en vue de favoriser l'harmonisation des législations nationales, sans que cela exclue l'établissement ultérieur d'une convention internationale. Ces travaux devaient s'effectuer en coopération étroite avec le Conseil de l'Europe et la Communauté Européenne et s'achever d'ici au 1er juillet 1979.

19. Le Groupe d'experts, placé sous la présidence de M. Kirby (Australie), et avec le concours de M. Peter Seipel (Consultant) a établi plusieurs projets et examiné divers rapports contenant notamment des analyses comparatives de diverses démarches adoptées à l'égard de la législation dans ce domaine. Il s'est attaché en particulier à un certain nombre de questions clés exposées ci-après :

- a) La question spécifique des faits de caractère sensible. En premier lieu, il s'agit de savoir si les lignes directrices devraient être de nature générale ou si elles devraient être structurées de manière à porter sur différents types de données ou d'activités (enquêtes de solvabilité, par exemple). En fait, il n'est probablement pas possible de définir un ensemble de données qui soient universellement considérées comme sensibles.
- b) La question du traitement automatique des données. L'argument selon lequel le traitement automatique de l'information constitue le principal motif de préoccupation est discutable et, en fait, contesté.
- c) La question des personnes morales. Certaines législations nationales, mais en aucun cas la totalité de celles-ci, assurent la protection des données relatives aux personnes morales de façon analogue à celle des données relatives aux personnes physiques.
- d) La question des voies de recours et des sanctions. Les démarches adoptées vis-à-vis des mécanismes de contrôle varient considérablement; c'est ainsi que l'on pourrait comparer les systèmes impliquant l'exercice d'une surveillance et la délivrance d'autorisations par des autorités spécialement constituées à cet effet aux systèmes impliquant l'observation facultative des règles par les maîtres de fichier et le recours aux moyens judiciaires traditionnels offerts par les tribunaux.
- e) La question des mécanismes fondamentaux ou de la mise en oeuvre. Le choix des principes fondamentaux et leur degré approprié de précision soulève des difficultés. C'est ainsi que l'on peut s'interroger sur la mesure dans laquelle les questions de sécurité des données (protection des données contre les ingérences non-autorisées, l'incendie et d'autres faits analogues) devraient être considérées comme faisant partie intégrante du domaine de

la protection de la vie privée; les opinions peuvent diverger en ce qui concerne les limites à assigner dans le temps à la conservation des données ou les conditions requises pour leur effacement, et la même remarque s'applique aux prescriptions selon lesquelles les données doivent être pertinentes par rapport à des finalités déterminées. En particulier, il est difficile de tracer une ligne de démarcation claire entre le niveau des principes ou objectifs de base et les questions de « mécanisme » qui se situent à un niveau inférieur et dont il conviendrait de réserver la mise en oeuvre au plan intérieur.

- f) La question du choix de la législation applicable. Les problèmes liés au choix de la juridiction, au choix de la législation applicable et à la reconnaissance des jugements rendus à l'étranger se sont avérés complexes dans le contexte des mouvements transfrontières de données. Cependant, la question se pose de savoir si et dans quelle mesure on devrait s'efforcer à ce stade de proposer, dans les lignes directrices, des solutions n'ayant pas force exécutoire.
- g) La question des exceptions. De même, les opinions peuvent diverger quant à la question des exceptions. Sont-elles vraiment nécessaires? Dans l'affirmative, faudrait-il prévoir des catégories particulières d'exceptions ou assigner des limites générales aux exceptions ?
- h) La question du parti pris. Enfin, il existe un conflit intrinsèque entre la protection et la libre circulation à travers les frontières des données de caractère personnel. L'accent peut être mis sur l'un ou l'autre de ces aspects et il peut être difficile d'établir une distinction entre les intérêts en matière de protection de la vie privée et d'autres intérêts ayant trait aux échanges, à la culture, à la souveraineté nationale, notamment.

20. Au cours de ses travaux, le Groupe d'experts a maintenu d'étroits contacts avec les organes correspondants du Conseil de l'Europe. Il n'a ménagé aucun effort pour éviter d'introduire des différences inutiles entre les textes établis par les deux organisations; ainsi, l'ensemble des principes fondamentaux est à maints égards analogue. Il existe en revanche un certain nombre de différences. Pour commencer, les lignes directrices de l'OCDE n'ont pas de caractère obligatoire du point de vue juridique, alors que le Conseil de l'Europe a établi une Convention qui liera juridiquement les pays qui l'auront ratifiée. Cela implique à son tour que la question des exceptions a été traitée de façon plus détaillée par le Conseil de l'Europe. Quant au domaine d'application, la Convention du Conseil de l'Europe se rapporte principalement au traitement automatique des données de caractère personnel, alors que les lignes directrices dé l'OCDE s'appliquent aux données de caractère personnel qui présentent des dangers pour la vie privée et les libertés individuelles, quels que soient les méthodes et les mécanismes utilisés pour les manipuler. Quant au degré de précision, les principes fondamentaux de protection proposés par les deux organisations ne sont pas identiques et la terminologie employée diffère à certains égards. Le cadre institutionnel en vue de la poursuite de la coopération est traité plus en détail dans la Convention du Conseil de l'Europe que dans les lignes directrices de l'OCDE.

21. Le Groupe d'experts a également continué à coopérer avec la Commission des Communautés Européennes, comme le prévoyait son mandat.

II. LES LIGNES DIRECTRICES

A. OBJET ET PORTEE

Généralités

22. Le préambule de la Recommandation fait état des préoccupations fondamentales qui appellent une action. La Recommandation confirme l'engagement pris par les pays Membres de protéger la vie privée et les libertés individuelles et de respecter les flux transfrontières de données de caractère personnel.

23. Les lignes directrices énoncées dans l'annexe à la Recommandation, comportent cinq

parties. La Partie Un comprend un certain nombre de définitions et indique la portée des lignes directrices, en précisant qu'elles constituent des normes minimales. La Partie Deux énonce huit principes fondamentaux (paragraphes 7 à 14) concernant la protection de la vie privée et des libertés individuelles au niveau national. La Partie Trois porte sur les principes applicables au plan international, c'est-à-dire les principes ayant principalement trait aux relations entre pays Membres.

24. La Partie Quatre expose, en termes généraux, des moyens de mettre en oeuvre les principes fondamentaux énoncés dans les parties précédentes et stipule que ces principes devraient être appliqués sans aucune discrimination. La Partie Cinq traite des questions d'assistance mutuelle entre pays Membres, l'accent étant mis sur l'échange d'informations et sur la nécessité d'éviter les incompatibilités dans les procédures nationales en matière de protection des données de caractère personnel. Il y est fait mention, en dernier lieu, des questions concernant la législation applicable lorsque les flux de données de caractère personnel font intervenir plusieurs pays Membres.

Objectifs

25. L'essentiel des lignes directrices réside dans les principes exposés à la Partie Deux de l'Annexe. Il est recommandé aux pays Membres d'observer ces principes de manière à:

- a) faire accepter aux pays Membres certaines normes minimales de protection de la vie privée et des libertés individuelles eu égard aux données de caractère personnel;
- b) réduire au minimum les différences entre les règles et pratiques intérieures des pays Membres en la matière;
- c) veiller à prendre en considération, dans la protection des données de caractère personnel, les intérêts d'autres pays Membres et la nécessité d'éviter des ingérences injustifiées dans les flux de données de caractère personnel entre pays Membres;
- d) éliminer dans la mesure du possible, les raisons qui pourraient inciter les pays Membres à restreindre les flux tranfrontières de données de caractère personnel à cause des risques éventuels liés à ces flux.

Comme il est indiqué dans le préambule, deux valeurs fondamentales jouent un rôle essentiel en l'occurrence : la protection de la vie privée et des libertés individuelles et le développement de la libre circulation des données de caractère personnel. Les lignes directrices visent à concilier ces deux valeurs; tout en admettant certaines restrictions à la libre circulation des données de caractère personnel à travers les frontières, elles cherchent à diminuer la nécessité de telles restrictions et, partant, à renforcer la notion de libre circulation de l'information entre pays.

26. Enfin, les Partes Quatre et Cinq des lignes directrices contiennent des principes qui ont pour objet :

- a) d'assurer la mise en oeuvre, à l'échelon national, de mesures efficaces pour la protection de la vie privée et des libertés individuelles;
- b) d'éviter les pratiques impliquant une discrimination inéquitable entre personnes physiques;
- c) de jeter les bases d'une coopération internationale suivie et de procédures compatibles dans le cadre de toute réglementation des flux transfrontières de données de caractère personnel.

Degré de précision

27. Le degré de précision des lignes directrices varie selon deux principaux facteurs, à savoir, (a) la mesure dans laquelle on est parvenu à un consensus au sujet des solutions proposées et (b) les connaissances et l'expérience dont on dispose pour déterminer les

solutions à adopter à ce stade. C'est ainsi que le principe de la participation individuelle (paragraphe 13) traite spécifiquement de divers aspects de la protection des intérêts des personnes physiques, alors que la disposition relative aux problèmes soulevés par le choix de la législation et aux questions connexes (paragraphe 22) ne fait qu'énoncer un point de départ pour l'élaboration progressive de méthodes communes et d'accords internationaux dans des domaines précis. Dans l'ensemble, les lignes directrices constituent un cadre général dans lequel les pays Membres pourront mener des actions concertées : les objectifs proposés par les lignes directrices pourront être réalisés de différentes manières, suivant les instruments juridiques et les stratégies que les pays Membres préféreront adopter pour leur mise en oeuvre. En conclusion, il est nécessaire que les lignes directrices fassent l'objet d'un examen suivi de la part des pays Membres comme de l'OCDE. Ce n'est que lorsque l'on aura acquis de l'expérience qu'il pourra s'avérer souhaitable de développer et d'adapter ces lignes directrices en conséquence.

Pays non membres

28. La Recommandation s'adresse aux pays Membres, comme il ressort de plusieurs dispositions expressément limitées aux relations entre pays Membres (voir paragraphes 15, 17 et 20 des lignes directrices). Cependant, il serait souhaitable que les lignes directrices soient largement admises et aucune de leurs dispositions ne devrait être interprétée comme empêchant l'application des dispositions pertinentes par les pays Membres à des pays non membres. Compte tenu de l'intensification des flux transfrontières de données et de la nécessité de garantir l'adoption de solutions concertées, on s'efforcera de porter les lignes directrices à l'attention des pays non membres et des organisations internationales compétentes en la matière.

Le contexte réglementaire élargi

29. Il a déjà été signalé que la protection de la vie privée et des libertés individuelles ne constitue que l'un des nombreux aspects juridiques du traitement de l'information qui se recoupent mutuellement. Les lignes directrices sont un instrument nouveau s'ajoutant à d'autres instruments internationaux connexes qui régissent des questions telles que les droits de l'homme, les télécommunications, les échanges internationaux, les droits d'auteur et divers services d'information. Si le besoin s'en faisait sentir, il serait possible dans le cadre des activités entreprises par l'OCDE eu égard aux politiques de l'information, de l'informatique et des communications, d'élargir encore les principes énoncés dans les lignes directrices.

30. Certains pays Membres ont fait valoir les avantages qu'offrirait une convention internationale de vaste portée ayant force exécutoire. Au terme de son mandat, le Groupe d'experts avait pour mission d'élaborer les lignes directrices relatives aux règles fondamentales régissant le mouvement transfrontière de données de caractère personnel et la protection des libertés individuelles, sans que cela exclue l'établissement ultérieur d'une convention internationale de nature obligatoire. Les lignes directrices pourraient servir de point de départ à l'élaboration d'une convention internationale lorsque la nécessité en apparaîtra.

Personnes morales, groupes et entités analogues

31. De l'avis de certains pays, la protection à accorder aux données relatives aux personnes physiques peut être de même nature que celle requise pour les données concernant les entreprises industrielles et commerciales, les associations et groupes qui peuvent ou non être dotés de la personnalité juridique. L'expérience acquise par un certain nombre de pays montre aussi qu'il est difficile de tracer clairement la ligne de démarcation entre les données de caractère personnel et celles qui ne le sont pas. Les données relatives à une petite entreprise, par exemple, peuvent également concerner son (ou ses) propriétaire(s) et fournir des informations de caractère personnel plus ou moins sensibles. Dans de tels cas, il pourra être souhaitable d'étendre aux organismes constitués en sociétés la protection offerte

par des règles qui se rapportent principalement aux données de caractère personnel.

32. De même, on peut s'interroger sur la mesure dans laquelle les personnes appartenant à un groupe particulier (handicapés mentaux, immigrants, minorités ethniques, par exemple) doivent bénéficier d'une protection supplémentaire contre la diffusion d'informations concernant ledit groupe.

33. En revanche, les lignes directrices reflètent le point de vue selon lequel les notions d'intégrité individuelle et de vie privée sont à maints égards particulières et ne devraient pas être traitées de la même manière que l'intégrité d'un groupe de personnes ou la sécurité des sociétés et le caractère confidentiel de leurs activités. Les besoins de protection sont différents, de même que le cadre dans lequel les solutions doivent être formulées et les intérêts doivent être conciliés. Certains membres du Groupe d'experts ont suggéré que la faculté d'étendre les lignes directrices aux personnes morales (sociétés, associations) devrait être prévue. Cette suggestion n'ayant pas suscité un consensus suffisant, la portée des lignes directrices est donc limitée aux données concernant les personnes physiques, le soin étant laissé aux pays Membres de fixer des lignes de démarcation et d'arrêter les mesures ayant trait aux sociétés, groupes et organismes analogues (voir paragraphe 49 ci-après).

Traitement automatique et non automatique des données

34. Les activités que l'OCDE a consacrées dans le passé à la protection de la vie privée et à des domaines connexes étaient axées sur le traitement automatique de l'information et sur les réseaux d'ordinateurs. Le Groupe d'experts s'est particulièrement penché sur la question de savoir si la portée de ces lignes directrices devrait ou non être limitée au traitement automatique et informatisé des données de caractère personnel. Cette façon d'aborder le problème peut se justifier pour un certain nombre de raisons, comme les dangers particuliers que comportent, pour les libertés individuelles, l'automatisation et les banques de données informatisées, la prédominance croissante des méthodes de traitement automatique de l'information, notamment dans le contexte des flux transfrontières de données, et le cadre propre aux politiques de l'information, de l'informatique et des télécommunications, dans lequel le Groupe d'experts a entrepris de s'acquitter de son mandat.

35. Par ailleurs, le Groupe d'experts est parvenu à la conclusion que le fait de limiter la portée des lignes directrices au traitement automatique des données de caractère personnel aurait des inconvénients considérables. Tout d'abord, il est difficile, au niveau des définitions, d'établir une nette distinction entre le traitement automatique et non-automatique de l'information. Il existe, par exemple, des systèmes mixtes de traitement de l'information et certaines étapes du traitement de l'information qui peuvent ou non se prêter à l'automatisation. Ces difficultés sont encore souvent compliquées par les progrès techniques constants, tels que l'introduction de méthodes semi-automatiques perfectionnées reposant sur l'utilisation de micro-films ou de micro-ordinateurs, lesquels pourront être de plus en plus utilisés à des fins privées qui sont à la fois inoffensives et incontrôlables. De plus, si elles étaient uniquement axées sur les ordinateurs, les lignes directrices pourraient donner lieu à des incohérences et des lacunes, de même qu'elles pourraient fournir aux maîtres de fichier des possibilités de se soustraire aux règles portant application des lignes directrices en utilisant des moyens non-automatiques à des fins susceptibles d'être nuisibles.

36. En raison des difficultés évoquées, les lignes directrices n'énoncent pas de définition du « traitement automatique des données » bien que le préambule et le paragraphe 3 de l'Annexe s'y réfèrent. On peut admettre que, pour l'interprétation de cette notion, il est possible de s'inspirer de sources telles que les vocabulaires techniques classiques.

37. On peut surtout faire valoir que les principes relatifs à la protection de la vie privée et des libertés individuelles exposés dans les lignes directrices sont applicables au traitement de l'information en général, quelle que soit la technologie particulière employée. En conséquence, les lignes directrices s'appliquent aux données de caractère personnel en

général ou, plus précisément, aux données de caractère personnel qui, en raison de la façon dont elles sont traitées, de leur nature ou de leur contexte, comportent un danger pour la vie privée et les libertés individuelles.

38. Il conviendrait toutefois de noter que les lignes directrices ne constituent pas un recueil de principes généraux applicables à la protection de la vie privée ; les intrusions dans la vie privée, comme la prise de photographies à l'insu du sujet, les mauvais traitements physiques ou la diffamation, par exemple, sortent de leur champ d'application, à moins que ces actes ne soient d'une manière ou d'une autre liés à la manipulation de données de caractère personnel Ainsi, les lignes directrices visent la constitution et l'utilisation d'ensembles de données qui sont organisées en vue de leur saisie, de la prise de décisions, de recherches, d'enquêtes et à des fins analogues. Il y aurait lieu de souligner que les lignes directrices sont neutres en ce qui concerne la technologie particulière utilisée; les méthodes automatiques ne constituent que l'un des problèmes évoqués dans les lignes directrices, bien que, notamment dans le contexte des flux transfrontières de données, il s'agisse manifestement d'un problème important.

B. COMMENTAIRES DETAILLES

Généralités

39. Les commentaires formulés ci-après se rapportent au texte même des lignes directrices figurant en annexe à la Recommandation. Ils ont pour objet de préciser le sens des débats qui ont eu lieu au sein du Groupe d'experts.

Paragraphe 1 : Définitions

40. On a fait en sorte que la liste des définitions soit brève. Le terme « maître du fichier » revêt une importance capitale. Il vise à définir la personne qui, en vertu du droit interne, devrait assumer en dernier ressort la responsabilité des activités ayant trait au traitement de données de caractère personnel. Selon la définition qui en est donnée, le maître du fichier est une personne qui est habilitée à décider du contenu et de l'utilisation des données, que ces données soient ou non collectées, enregistrées, traitées ou diffusées par ladite personne ou par un agent agissant en son nom. Le maître du fichier peut être une personne morale ou physique, une autorité publique, une agence ou tout autre organisme. Sont exclues de cette définition au moins quatre catégories de personnes morales et physiques susceptibles d'intervenir dans le traitement de l'information, à savoir :

- (a) les autorités chargées de délivrer des autorisations et les organismes analogues existant dans certains pays Membres qui autorisent le traitement de l'information mais ne sont pas habilités à décider (au sens propre du terme) quelles activités devraient être exercées et à quelles fins ;
- (b) les centres de traitement à façon qui procèdent au traitement des données au nom de tiers ;
- (c) les autorités compétentes en matière de télécommunications et les organismes analogues qui jouent simplement le rôle de voie de transmission et
- (d) les « utilisateurs dépendants » qui peuvent avoir accès aux données mais ne sont pas autorisés à décider quelles données devraient être enregistrées, qui devrait être en mesure de les utiliser, etc. Lors de la mise en oeuvre des lignes directrices, les pays pourront élaborer des dispositifs plus complexes fixant les divers niveaux et types de responsabilités.

Les paragraphes 14 et 19 des lignes directrices pourront servir de base aux efforts qui seront entrepris dans ce sens.

41. Les termes « données de caractère personnel » et « personne concernée » ont pour objet de souligner que les lignes directrices visent les personnes physiques. Il peut être

difficile de tracer la ligne de démarcation précise entre les données de caractère personnel au sens de l'information relative à des personnes identifiées ou identifiables et les données anonymes, et c'est à la réglementation de chaque pays Membre qu'il appartiendra de le faire. En principe, les données de caractère personnel transmettent une information qui, par des liaisons directes (numéro matricule civil, par exemple) peut être rattachée à une personne physique particulière.

42. Le terme « flux transfrontières de données de caractère personnel »limite l'application de certaines dispositions des lignes directrices aux flux internationaux de données et, en conséquence, ne tient pas compte des problèmes de flux de données propres aux Etats fédéraux. Les mouvements de données s'effectueront souvent par l'intermédiaire de la transmission électronique mais pourront également emprunter d'autres moyens de transmission. Au sens des présentes lignes directrices, les flux transfrontières englobent la transmission des données par satellite.

Paragraphe 2 : Champ d'application

43. La section de l'Exposé relative à l'objet et à la portée des lignes directrices pose la question de leur application au traitement automatique des données de caractère personnel, par opposition à leur traitement non automatique. Le paragraphe 2 des lignes directrices, qui traite de ce problème, se fonde sur deux critères limitatifs. Le premier est associé à la notion de données de caractère personnel : les lignes directrices s'appliquent aux données qui peuvent être rattachées à des personnes physiques identifiées ou identifiables. Les opérations de collecte des données qui n'offrent pas de telles possibilités (collecte de données statistiques sous une forme anonyme) en sont exclues. Le second critère, plus complexe, est lié à un élément de risques spécifiques de nature concrète, à savoir que les données comportent un danger pour la vie privée et les libertés individuelles. De tels dangers peuvent découler de l'utilisation des méthodes de traitement automatisé de l'information (façon dont les données sont traitées) mais il existe un large éventail d'autres sources de risques. Ainsi, les données qui sont, en soi, simples et concrètes pourront être utilisées dans un contexte dans lequel elles deviendront nuisibles à une personne concernée. En revanche les risques tels qu'ils sont exposés au paragraphe 2 des lignes directrices, visent à exclure les opérations de collecte de données de nature manifestement inoffensives (agendas personnels, par exemple). Les dangers évoqués au paragraphe 2 des lignes directrices devraient se rapporter à la vie privée et aux libertés individuelles. Cependant les intérêts protégés ont une large portée (voir paragraphe 2 ci-dessus) et pourront être envisagés de façons différentes suivant les pays et les époques. Les principes énoncés dans les paragraphes 7 à 13 indiquent les limitations propres aux lignes directrices et définissent une méthode fondamentale commune.

44. Comme il est précisé au paragraphe 2 des lignes directrices, celles-ci visent à couvrir aussi bien le secteur privé que le secteur public. Ces notions pourront être définies différemment suivant les pays Membres.

Paragraphe 3 : Différents degrés de sensibilité

45. Les lignes directrices ne devraient pas être appliquées de façon mécanique, quels que soient les types de données et d'activités de traitement en cause. Le cadre offert par les principes fondamentaux énoncés dans la Partie Deux des lignes directrices permet aux pays Membres d'exercer leur pouvoir discrétionnaire eu égard à la rigueur avec laquelle les lignes directrices doivent être appliquées et à la portée des mesures à prendre. En particulier, aux termes de l'alinéa 3(b), de nombreux cas « insignifiants » de collecte et d'utilisation des données de caractère personnel (voir ci-dessus) seront entièrement exclus du champ d'application des lignes directrices. Manifestement, cela ne signifie pas que le paragraphe 3 devrait être considéré comme un instrument destiné à saper les normes fixées par les lignes directrices. Mais, dans l'ensemble, les lignes directrices ne sont pas supposées être mises en oeuvre de façon uniforme par les pays Membres au niveau des détails. Par exemple, il faut

tenir compte des traditions différentes et des attitudes différentes du public. Ainsi, dans un certain pays, les identificateurs individuels universels pourront être considérés comme inoffensifs et utiles alors que, dans un autre pays, ils pourront être considérés comme éminemment délicats et leur utilisation pourra être limitée, voire interdite. Dans un certain pays, la protection pourra être accordée aux données concernant des groupes en entités analogues alors que, dans un autre, cette protection sera totalement inexistante, etc. En conclusion, il se peut que quelques pays Membres jugent bon de limiter l'application des lignes directrices au traitement automatique des données de caractère personnel. L'alinéa 3(c) prévoit une telle limitation.

Paragraphe 4 : Exceptions aux lignes directrices

46. Il peut sembler superflu de prévoir explicitement des exceptions dans les lignes directrices qui font partie d'une Recommandation n'ayant pas force exécutoire. Cependant, le Groupe d'experts a jugé opportun d'insérer à ce sujet une disposition stipulant que deux critères généraux devraient orienter l'action susceptible d'être menée au plan national pour limiter l'application des lignes directrices. Les exceptions devraient être aussi peu nombreuses que possible et être portées à la connaissance du public (notamment par voie de publication dans le Journal Officiel). La connaissance générale de l'existence de certaines données ou fichiers serait suffisante pour satisfaire le deuxième critère, encore que des détails concernant des données particulières etc. puissent devoir être gardés secrets. La formule retenue au paragraphe 4, bien que brève, a pour objet de couvrir de nombreux types de préoccupations et de facteurs limitatifs, car il n'est manifestement pas possible de fournir une liste exhaustive d'exceptions -- d'où l'introduction de l'expression « y compris celles intéressant la souveraineté nationale, la sécurité nationale et l'ordre public ». Une autre préoccupation nationale primordiale concerne par exemple le crédit public. En outre, le paragraphe 4 prévoit différentes façons de mettre en oeuvre les lignes directrices ; il ne faudrait pas perdre de vue que les pays Membres ont actuellement atteint différents stades eu égard à la mise en place de règles et institutions destinées à assurer la protection de la vie privée et qu'ils vont vraisemblablement progresser à des rythmes différents en appliquant des stratégies différentes, telles que la réglementation de certains types de données ou d'activités par opposition à une réglementation d'ordre général (« méthode globale »).

47. Le Groupe d'experts a reconnu que les pays Membres pourraient appliquer de façon différenciée les lignes directrices à divers types de données de caractère personnel. Des différences pourront se produire dans la fréquence admissible des inspections, dans les façons de concilier des intérêts antagonistes, tels que le caractère confidentiel des dossiers médicaux en regard du droit, de la personne physique de vérifier les données la concernant, etc. L'évaluation de la solvabilité, la sûreté nationale et le secteur bancaire constituent quelques exemples de domaines qui peuvent être traités différemment. Les pays Membres pourront également opter pour des solutions différentes en ce qui concerne les exceptions liées à la recherche et aux statistiques, par exemple. Une énumération exhaustive de tous ces cas et de toutes ces préoccupations n'est ni nécessaire ni possible. Certains des paragraphes figurant dans la suite des lignes directrices et les commentaires y afférents fournissent de nouveaux éclaircissements sur le champ d'application de ces dernières et sur les questions étroitement liées que pose la conciliation d'intérêts divergents (comparer avec les paragraphes 7, 8, 17 et 18 des lignes directrices). En résumé, le Groupe d'experts a admis que les exceptions se limiteront à celles qui s'imposent dans une société démocratique.

Paragraphe 5 : Pays à structure fédérale

48. Dans les pays à structure fédérale, l'application des lignes directrices est soumise à diverses limitations constitutionnelles. En conséquence, le paragraphe 5 sert à souligner qu'il n'existe aucun engagement d'appliquer les lignes directrices hors du cadre des compétences

constitutionnelles.

Paragraphe 6 : Normes minimales

49. En premier lieu, le paragraphe 6 assimile les lignes directrices à des normes minimales devant être adoptées dans le droit interne. En deuxième lieu et par voie de conséquence, il a été convenu que les lignes directrices sont susceptibles d'être complétées par d'autres mesures visant à protéger la vie privée et les libertés individuelles à l'échelon aussi bien national qu'international.

Paragraphe 7 : Principe de la limitation en matière de collecte

50. Il y aurait lieu de faire remarquer, en guise d'introduction aux principes énoncés dans les paragraphes 7 à 14 des lignes directrices, que ces principes sont interdépendants et se recouvrent partiellement. Ainsi, les distinctions qui sont admises dans les principes entre différentes activités et étapes du traitement de l'information, sont quelque peu artificielles et il est essentiel que les principes soient abordés conjointement et étudiés comme un tout. Le paragraphe 7 se rapporte à deux questions, à savoir :

- (a) les limites à la collecte des données qui, en raison de la façon dont elles seront traitées, de leur nature, du contexte dans lequel elles seront utilisées ou d'autres circonstances, sont considérées comme particulièrement sensibles et
- (b) les prescriptions relatives aux méthodes de collecte des données. Les opinions émises au sujet de la première question divergent fréquemment. On pourrait faire valoir qu'il est à la fois possible et souhaitable d'énumérer les types ou catégories de données qui sont en soi sensibles et dont la collecte devrait être limitée, voire interdite.

Il existe, dans la législation européenne, des précédents à cet effet (race, convictions religieuses, casier judiciaire par exemple). En revanche, on peut soutenir qu'aucune donnée est en elle-même de nature privée ou sensible, mais peut le devenir selon son contexte et l'utilisation qui en est faite. Cette opinion se reflète notamment dans la législation des Etats-Unis relative à la protection de la vie privée.

51. Le Groupe d'experts a examiné un certain nombre de critères de sensibilités, tels que le risque de discrimination, mais a estimé qu'il n'était pas possible de définir un ensemble de données qui soient universellement tenues pour sensibles. En conséquence, le paragraphe 7 contient simplement une déclaration générale, selon laquelle des limites devraient être assignées à la collecte des données de caractère personnel. Il s'agit là, tout d'abord, d'une recommandation affirmative à l'intention du législateur pour l'inciter à fixer des limites qui mettraient fin à la collecte sans discernement des données de caractère personnel. La nature des limites peuvent concerner:

- les aspects qualitatifs des données (c'est-à-dire qu'il devrait être possible de tirer des données collectées une information de suffisamment bonne qualité, et que les données devraient être collectées dans un cadre informationnel approprié, etc.);
- la finalité du traitement de l'information (c'est-à-dire que seules certaines catégories de données devraient être collectées et, si possible, que les données collectées devraient être limitées à celles qui sont strictement nécessaires pour atteindre la finalité spécifiée);
- le « marquage » de données particulièrement sensibles selon les traditions et les attitudes propres à chaque pays Membre;
- les activités de collecte des données de certains maîtres de fichier;
- les préoccupations liées aux droits civiques.

52. La deuxième partie du paragraphe 7 (méthode de collecte des données) vise à empêcher les pratiques impliquant, par exemple, l'utilisation de dispositifs secrets d'enregistrement des données, tels que les magnétophones, ou les manoeuvres destinées à induire la

personne concernée en erreur pour en obtenir des informations. La nécessité de porter les données à la connaissance de la personne concernée ou d'obtenir le consentement de cette dernière est une règle essentielle, cette connaissance constituant l'exigence minimale. En revanche, il n'est pas toujours possible, pour des raisons pratiques, d'imposer l'obtention du consentement. En outre, le paragraphe 7 rappelle également (« le cas échéant ») qu'il existe certains cas où, pour des raisons pratiques ou de principe, on peut ne pas juger nécessaire de porter les données à la connaissance de la personne concernée ou d'obtenir son consentement. Les enquêtes criminelles et la mise à jour courante des listes de distribution peuvent servir d'exemples à cet égard. Enfin, le paragraphe 7 n'exclut pas la possibilité, pour une personne concernée, de se faire représenter par une tierce partie, par exemple dans le cas des mineurs, des handicapés mentaux, etc.

Paragraphe 8 : Principe de la qualité de l'information

53. On peut envisager de façon différente les prescriptions selon lesquelles les données doivent être pertinentes. En fait, certains membres du Groupe d'experts ont marqué certaines hésitations sur le point de savoir si de telles prescriptions entrent effectivement dans le cadre de la protection de la vie privée. Le Groupe d'experts est toutefois parvenu à la conclusion qu'il convient de rattacher les données à la finalité en vue de laquelle elles seront utilisées. C'est ainsi que les données concernant des opinions peuvent facilement induire en erreur si elles sont utilisées à des fins avec lesquelles elles n'ont pas de rapport et la même remarque s'applique aux données d'évaluation. Le paragraphe 8 traite également de l'exactitude, de l'exhaustivité et de la mise à jour qui sont autant d'éléments importants couverts par la notion de qualité de' l'information. Les prescriptions à cet égard sont liées aux finalités des données, c'est-à-dire que leur portée ne devrait pas dépasser celle requise pour les finalités en vue desquelles les données sont utilisées. Ainsi, les données historiques peuvent souvent devoir être collectées ou conservées ; il s'agit en l'occurrence des recherches en sciences sociales impliquant des études dites longitudinales de l'évolution de la société, des recherches historiques et des activités d'archivage. Le « critère de finalité » amènera souvent à se demander si un dommage peut ou non être causé aux personnes concernées en raison du manque d'exactitude, d'exhaustivité et de mise à jour.

Paragraphe 9 : Principe de la spécification des finalités

54. Le principe de la spécification des finalités est étroitement associé aux deux principes qui l'entourent, c'est-à-dire le principe de la qualité des données et celui de la limitation de l'utilisation. Fondamentalement le paragraphe 9 implique qu'avant ou, en tout cas, au plus tard au moment de la collecte des données, il devrait être possible de déterminer les finalités en vue desquelles ces données seront utilisées et que les modifications ultérieures de finalités devraient être spécifiées de la même façon. Ces finalités peuvent être spécifiées d'un certain nombre de manières différentes ou complémentaires, et notamment par des déclarations publiques, l'information des personnes concernées, la législation, les décrets administratifs, et les autorisations délivrées par des organes de tutelle. En vertu des paragraphes 9 et 10, de nouvelles finalités ne devraient pas intervenir de façon arbitraire; la liberté d'apporter des modifications devrait impliquer la compatibilité avec les finalités initiales. Enfin, lorsque les données n'auront plus de finalité et si cela est possible, il pourra être nécessaire de les faire détruire (effacer) ou de leur conférer une forme anonyme. La raison en est que, lorsque les données ne présentent plus d'intérêt, il arrive que l'on en perde le contrôle, ce qui peut entraîner des risques de vol, de reproduction non-autorisée ou autres actes illicites.

Paragraphe 10 : Principe de la limitation de l'utilisation

55. Ce paragraphe a trait aux utilisations de différents types, y compris la divulgation, qui impliquent des écarts par rapport aux finalités spécifiées. C'est ainsi que les données pourront être transmises d'un ordinateur à un autre et utilisées en vue de finalités non-autorisées sans être vérifiées et, partant, divulguées au sens propre du terme. En règle

générale, les finalités spécifiées à l'origine ou ultérieurement devraient jouer un rôle décisif dans les utilisations qui pourront être faites des données. Le paragraphe 10 prévoit deux exceptions générales à ce principe qui s'énoncent comme suit : « avec le consentement de la personne concernée » (ou de son représentant - cf. paragraphe 52 ci-dessus) ou lorsqu'une règle de droit le prévoit (notamment dans le cas des autorisations délivrées par des organes de tutelle). On peut par exemple prévoir que les données ayant été collectées en vue de la prise de décisions d'ordre administratif, sont susceptibles d'être fournies à des fins de recherche, de statistiques et de planification sociale.

Paragraphe 11 : Principe des garanties de sécurité

56. Les notions de sécurité et de protection de la vie privée n'ont pas la même signification. Cependant, les limitations imposées à l'utilisation et à la divulgation des données devraient être renforcées par des garanties de sécurité. Ces garanties comprennent des mesures d'ordre matériel (verrouillage des portes et cartes d'identification, par exemple), des mesures structurelles (telles que les niveaux hiérarchiques en ce qui concerne l'accès aux données) et, en particulier avec les systèmes informatiques, des mesures informationnelles (telles que le chiffrement et la surveillance des activités inhabituelles susceptibles de présenter un danger et des mesures destinées à y faire face). Il conviendrait de souligner que la catégorie des mesures structurelles comprend l'obligation faite au personnel chargé du traitement de l'information de maintenir le caractère confidentiel des données. Le paragraphe 11 a un champ d'application étendu. Les cas mentionnés dans cette disposition se chevauchent dans une certaine mesure (accès/divulgation, par exemple). La « perte » de données recouvre notamment l'effacement accidentel de données, la destruction de supports d'information (et, partant, la destruction de données) et le vol de supports d'information. Le mot « modification » devrait être interprété comme englobant l'entrée non-autorisée de données et le mot « utilisation », comme englobant la reproduction non-autorisée de données.

Paragraphe 12 : Principe de la transparence

57. Le principe de la transparence peut être considéré comme une condition préalable au principe de la participation individuelle (paragraphe 13) ; pour que ce dernier puisse être appliqué de façon efficace, il doit être possible dans la pratique d'acquérir des informations sur la collecte, l'enregistrement ou l'utilisation des données de caractère personnel. La communication régulière, à titre facultatif d'informations par les maîtres de fichier, la publication dans des registres officiels de descriptions des activités relatives au traitement des données de caractère personnel et l'inscription auprès d'organismes publics constituent quelques-uns, mais non pas la totalité, des moyens qui permettraient d'atteindre cet objectif. La référence aux moyens qu'il devrait être « possible de se procurer aisément » implique que les personnes physiques devraient être en mesure d'obtenir des informations sans effort déraisonnable eu égard aux délais, à la connaissance préalable, aux déplacements, etc., et sans coût déraisonnable.

Paragraphe 13 : Principe de la participation individuelle

58. Le droit des personnes physiques d'avoir accès aux données de caractère personnel et de les contester est, en règle générale, considéré comme étant peut-être la principale garantie de protection de la vie privée. Ce point de vue est partagé par le Groupe d'experts qui, tout en étant conscient du fait que le droit d'accès et de contestation ne saurait être absolu, a décidé de l'exprimer en des termes clairs et assez précis. Les différents alinéas de ce paragraphe appellent les explications suivantes :

59. Le droit d'accès devrait, en règle générale, être simple à exercer. Cela peut signifier notamment qu'il devrait s'inscrire dans le cadre des activités quotidiennes du maître du fichier ou de son représentant et ne nécessiter aucune action juridique ou mesure analogue. Parfois, il y aurait peut-être lieu de prévoir un accès intermédiaire aux données; dans le domaine médical, par exemple, le médecin pourra servir d'intermédiaire. Dans certains

pays, les organes de tutelle, tels que les autorités chargées de l'inspection des données, pourront assurer des services analogues. Il existe différentes manières de se conformer à la prescription selon laquelle les données devraient être communiquées dans des délais raisonnables. C'est ainsi qu'un maître de fichier qui fournit des informations aux personnes concernées à intervalles réguliers pourra être dispensé de l'obligation de répondre immédiatement aux demandes présentées à titre individuel. Normalement, le délai doit être compté à partir de la réception d'une demande. Sa durée pourra varier dans une certaine mesure d'un cas à l'autre, en fonction de circonstances telles que la nature de l'activité de traitement de l'information. Par transmission des données « selon des modalités raisonnables », on entend notamment que les problèmes de distance géographique devraient être dûment pris en considération. De plus, si des intervalles sont prescrits entre les moments où les demandes d'accès doivent être satisfaites, il faudrait que ces intervalles soient raisonnables. La mesure dans laquelle les personnes concernées devraient pouvoir obtenir des copies des données les concernant est une question de mise en oeuvre qu'il appartiendra à chaque pays Membre de régler.

60. Le droit d'être informé des raisons mentionné à l'alinéa 13 (c) est restreint, en ce sens qu'il est limité à des cas où les demandes d'information ont été rejetées. L'idée d'élargir ce droit de manière à englober les raisons pour lesquelles des décisions défavorables en général seraient prises sur la base de données de caractère personnel a suscité une réaction favorable au sein du Groupe d'experts. Cependant, lors de l'examen final, on a estimé qu'un droit de cette nature est de trop vaste portée pour pouvoir figurer dans le cadre des principes de protection de la vie privée que constituent les lignes directrices. Cela ne veut pas dire que le droit d'être informé des raisons pour lesquelles une décision favorable aurait été prise, puisse ne pas être opportun par exemple pour informer et alerter une personne concernée à propos de ses droits, afin quelle puisse les exercer effectivement.

61. Le droit de contester visé aux alinéas 13 (c) et (d), qui a une large portée, couvre les contestations introduites en premier lieu devant le maître du fichier, de même que les contestations présentées ultérieurement devant les tribunaux, organismes administratifs, organes professionnels ou autres institutions suivant les règlements intérieurs des pays (comparer avec le paragraphe 19 des lignes directrices). Le droit de contester ne signifie pas que la personne concernée peut décider quels recours ou quelles réparations sont disponibles (rectification, introduction d'une mention précisant que les données font l'objet de litiges, etc...) : ces questions seront tranchées en vertu du droit interne et des procédures juridiques intérieures. En termes généraux, les critères qui régissent l'issue d'une contestation sont ceux énoncés dans d'autres passages des lignes directrices.

Paragraphe 14 : Principe de la responsabilité

62. Le maître du fichier décide du choix des données et des activités de traitement de l'information. C'est pour son compte que les données sont traitées. En conséquence, il est essentiel qu'aux termes du droit interne la responsabilité, devant la loi, du respect des règles et des décisions concernant la protection de la vie privée incombe au maître du fichier, qui ne devrait pas être relevé de cette obligation pour la simple raison que le traitement des données est effectué pour son compte par un tiers, tel qu'un centre de traitement à façon. En revanche, rien dans les lignes directrices n'empêche de tenir également responsables le personnel des centres de traitement à façon, les « utilisateurs dépendants » et autres (voir paragraphe 40). C'est ainsi que les sanctions prises contre la non-observation de l'obligation de maintenir le caractère confidentiel pourront toucher toutes les personnes physiques ou morales chargées du traitement des données de caractère personnel (voir paragraphe 19 des lignes directrices). Au sens du paragraphe 14, il faut entendre, par responsabilité, la responsabilité assortie de sanctions juridiques, ainsi que la responsabilité établie en vertu de codes de déontologie, par exemple.

Paragraphes 15-18 : Principes fondamentaux applicables au plan international

63. Les principes fondamentaux applicables au plan international sont étroitement interdépendants. En termes généraux, le paragraphe 15 concerne le respect par les pays Membres de leurs intérêts réciproques en matière de protection des données de caractère personnel, de même que la vie privée et des libertés individuelles de leurs ressortissants et résidents. Le paragraphe 16 traite des questions de sécurité au sens large du terme et on peut dire qu'il correspond, à l'échelon international, au paragraphe 11 des lignes directrices. Les paragraphes 17 et 18 portent sur les restrictions imposées à la libre circulation des données de caractère personnel entre pays Membres; fondamentalement, en ce qui concerne la protection de la vie privée et des libertés individuelles, ces flux transfrontières devraient être admis dès lors que les prescriptions des lignes directrices relatives à la protection desdits intérêts ont été remplies en substance, c'est-à-dire effectivement. La question des autres motifs susceptibles de justifier des restrictions aux flux transfrontières de données de caractère personnel, n'est pas traitée dans les lignes directrices.

64. Le paragraphe 15 a deux conséquences pour le traitement de l'information au plan intérieur. D'une part, il a pour objet d'empêcher les politiques libérales qui sont contraires à l'esprit des lignes directrices et facilitent les tentatives visant à tourner ou à violer la législation d'autres pays Membres en matière de protection. Toutefois, de telles tentatives bien qu'elles soient condamnées par tous les pays Membres, ne sont pas spécifiquement mentionnées dans ce paragraphe, car un certain nombre de pays estiment qu'il est inadmissible qu'un pays Membre soit tenu de mettre en oeuvre directement ou indirectement, sans rattachement territorial, la législation d'autres pays Membres. Il conviendrait de remarquer que la disposition mentionne explicitement la réexportation des données de caractère personnel. A cet égard, les pays Membres ne devraient pas perdre de vue la nécessité de se soutenir réciproquement dans leurs efforts en vue de s'assurer que les données de caractère personnel ne cessent pas d'être protégées du fait de leur transfert, en vue du traitement de l'information, à des territoires et à des installations dans lesquels le contrôle est lâche ou inexistant.

65. D'autre part, les pays Membres sont implicitement encouragés à envisager la nécessité d'adapter les règles et pratiques de traitement de l'information aux circonstances particulières qui peuvent se présenter lorsque des données d'origine étrangère et des données concernant des étrangers sont en cause. A titre d'exemple, il peut arriver que des données relatives à des cibles ressortissants étrangers soient rendues disponibles à des fins qui répondent aux intérêts particuliers de leur pays d'origine (par exemple, accès aux adresses de ressortissants vivant à l'étranger).

66. En ce qui concerne les lignes directrices, l'encouragement des flux internationaux de données de caractère personnel n'est pas un but incontesté en soi. Dans la mesure où de tels flux se produisent, ils devraient toutefois, en vertu du paragraphe 16, avoir lieu sans interruption et en toute sécurité, c'est-à-dire être protégés contre un accès non-autorisé, la perte de données et des circonstances analogues. Cette protection devrait également être accordée aux données en transit, c'est-à-dire aux données qui passent a travers un pays Membre sans être utilisées ou stockées en vue de leur emploi dans ce pays. L'engagement général visé au paragraphe 16 devrait, pour ce qui est des réseaux d'ordinateurs, être considéré dans le contexte de la Convention internationale des télécommunications de Malaga-Torremolinos (25 octobre 1973). En vertu de cette Convention, les membres de l'Union Internationale des Télécommunications (UIT), y compris les pays Membres de l'OCDE, sont convenus notamment de prendre les mesures utiles en vue d'établir, dans les meilleures conditions techniques, les voies et installations nécessaires pour assurer l'échange rapide et ininterrompu des télécommunications internationales. En outre, les membres de l'UIT sont convenus de prendre toutes les mesures possibles, compatibles avec le système de télécommunication employé, en vue d'assurer le secret des correspondances internationales. Quant aux exceptions, les membres se sont réservé le droit de suspendre le service des télécommunications internationales, de même que le droit de communiquer les

correspondances internationales aux autorités compétentes, afin d'assurer l'application de leur législation intérieure ou l'exécution des conventions internationales auxquelles les pays Membres de l'UIT sont parties. Ces dispositions s'appliquent tant que les données sont acheminées par des lignes de télécommunication. Dans leur contexte, les lignes directrices constituent un moyen supplémentaire de garantir que les flux internationaux de données de caractère personnel ont lieu sans interruption et en toute sécurité.

67. Le paragraphe 17 vient renforcer le paragraphe 16 en ce qui concerne les relations entre pays Membres. Il traite également des intérêts qui sont opposés à la libre circulation, à travers les frontières, des données de caractère personnel mais qui peuvent néanmoins constituer des raisons légitimes de restreindre cette circulation entre pays Membres. A titre d'exemple caractéristique, on peut citer les tentatives visant à échapper à la législation nationale en effectuant des opérations de traitement de l'information dans un pays Membre qui ne se conforme pas encore réellement aux lignes directrices. Le paragraphe 17 établit une norme de protection équivalente, c'est-à-dire protection dont l'effet est pour l'essentiel semblable à celle du pays exportateur mais qui ne doit pas nécessairement être identique à celle-ci, ni dans la forme, ni à tous autres égards. Comme dans le paragraphe 15, la réexportation de données de caractère personnel est spécifiquement mentionnée -- le but étant, en l'occurrence, d'empêcher un pays Membre de chercher à contourner la législation d'autres pays Membres sur la protection de la vie privée. La troisième série de raisons d'imposer des restrictions légitimes, dont il est fait état au paragraphe 17, à propos des données de caractère personnel qui sont de nature particulière, vise le cas où d'importants intérêts des pays Membres pourraient être lésés. Cependant, dans l'ensemble, le paragraphe 17 est assujetti aux dispositions du paragraphe 4 des lignes directrices selon lesquelles les restrictions imposées aux flux de données de caractère personnel devraient demeurer aussi peu nombreuses que possible.

68. Le paragraphe 18 a pour objet de concilier les intérêts liés à la protection de la vie privée et ceux liés à la libre circulation, à travers les frontières, des données de caractère personnel. Il vise avant tout à empêcher la création d'obstacles aux flux de données de caractère personnel qui seraient artificiels du point de vue de la protection de la vie privée et des libertés individuelles et poursuivraient des objectifs restrictifs d'autres types qui ne seraient donc pas déclarés. Cependant, le paragraphe 18 n'est pas destiné à limiter les droits des pays Membres de réglementer le mouvement transfrontière de données de caractère personnel dans des domaines ayant trait à la liberté des échanges, aux tarifs douaniers, à l'emploi et aux conditions économiques connexes applicables à la circulation internationale des données. Il s'agit de questions qui n'ont pas été abordées par le Groupe d'experts car elles sortent du cadre de son mandat.

Paragraphe 19 : Mise en oeuvre des principes à l'échelon national

69. Il appartient en premier lieu aux pays Membres de fixer les modalités détaillées d'application des Parties Deux et Trois des lignes directrices. Ces modalités vont nécessairement varier selon les différents régimes et traditions juridiques et le paragraphe 19 s'efforce donc simplement d'établir un cadre général exposant dans ses grandes lignes le type de mécanisme national qui est envisagé pour mettre les lignes directrices en application. La phrase liminaire esquisse les différentes façons dont les pays pourraient aborder la question tant sur un plan général qu'en ce qui concerne les mécanismes de contrôle (par exemple la création d'organes de tutelle spéciaux, le recours à des moyens de contrôle déjà en place, tels que tribunaux, autorités publiques, etc.).

70. Dans l'alinéa 19(a) les pays sont invités à adopter une législation intérieure appropriée, le mot « appropriée » préfigurant le jugement porté par les divers pays sur le caractère adéquat ou autre des solutions législatives. L'alinéa 19(b) relatif à l'autoréglementation, vise avant tout les pays de droit coutumier dans lesquels la mise en oeuvre par des voies non législatives des lignes directrices compléterait l'action législative. Il conviendrait de donner à

l'alinéa 19(c) une interprétation large; celui-ci prévoit des moyens tels que les avis formulés par les maîtres de fichier et la prestation d'une aide notamment juridique. L'alinéa 19(c) vise les sanctions pénales aussi bien que civiles et administratives. L'alinéa 19(d) permet d'aborder la question des mécanismes de contrôle de différentes façons ; il s'agit, en quelques mots, soit de créer des organes de tutelle spéciaux, soit de s'appuyer sur des moyens de contrôle déjà en place, que ce soient des tribunaux, des autorités publiques existantes ou d'autres organes. L'alinéa 19(e), qui porte sur la discrimination, vise à empêcher les pratiques inéquitables, mais il ménage la possibilité d'admettre une « discrimination bénigne » en vue d'aider des groupes défavorisés, par exemple. Cette disposition a pour objet d'empêcher la discrimination inéquitable qui serait notamment fondée sur la nationalité et le domicile, le sexe, la race, les croyances ou l'appartenance à des syndicats.

Paragraphe 20 : Echange d'informations et compatibilité des procédures

71. Deux principaux problèmes sont abordés en l'occurrence, à savoir : (a) la nécessité de faire en sorte que des informations puissent être obtenues sur les règles, réglementations, décisions, etc. portant application des lignes directrices ; et (b) la nécessité d'éviter que les flux transfrontières de données de caractère personnel ne soient entravés par un ensemble indûment complexe et disparate de procédures et de prescriptions de conformité. Le premier problème tient à la complexité des réglementations sur la protection de la vie privée et des politiques en matière de données en général. Il existe souvent plusieurs niveaux de réglementation (au sens large du terme) et nombre de règles importantes ne sauraient être fixées de façon permanente dans le cadre de dispositions statutaires détaillées ; il y a lieu de leur conserver un caractère assez souple et de les laisser à la discrétion des organes de décision de niveau inférieur.

72. L'importance du second problème est, en termes généraux, proportionnelle au nombre de législations intérieures qui concernent les flux transfrontières de données de caractère personnel. Même au stade actuel, il est manifestement nécessaire de coordonner dans les législations intérieures les dispositions spéciales sur les flux transfrontières de données, y compris des arrangements spéciaux, ayant trait au contrôle de conformité et, le cas échéant, aux autorisations d'exploiter des systèmes de traitement de l'information.

Paragraphe 21 : Mécanisme de coopération

73. La disposition relative aux procédures nationales part de l'hypothèse que les lignes directrices serviront de base à une coopération suivie. Les autorités chargées de la protection des données et les organismes spécialisés chargés de définir l'action gouvernementale dans le domaine de l'information et de la transmission des données sont manifestement associés dans le cadre d'une telle coopération. Le deuxième objectif de ces mesures en particulier, qui est énoncé à l'alinéa 21 (ii), soit l'assistance mutuelle lorsque des questions de procédure et des demandes d'informations sont en jeu, est orienté vers l'avenir et son importance pratique s'accroîtra probablement à mesure que les réseaux internationaux de données et les problèmes qu'ils posent deviendront plus nombreux et plus complexes.

Paragraphe 22 : Conflits de loi

74. Le Groupe d'experts a accordé une très grande attention aux problèmes de conflits de loi et, avant tout, à la question de savoir quels tribunaux devraient être compétents pour statuer sur des problèmes spécifiques (choix de la juridiction) et quel système juridique devrait régir des problèmes spécifiques (choix de la législation). L'examen de différentes stratégies et de divers principes proposés a confirmé le point de vue selon lequel, au stade actuel, étant donné la rapidité des progrès enregistrés au plan de la technologie, et compte tenu du caractère non exécutoire des lignes directrices, il n'y a pas lieu de tenter de proposer des solutions précises et détaillées. Des difficultés ne manqueront pas de se produire eu égard aussi bien au choix d'un modèle réglementaire valable du point de vue

théorique qu'à la nécessité d'acquérir une plus grande expérience des incidences des solutions qui, en soi, sont possibles.

75. Quant à la question du choix de la législation, l'une des façons d'aborder ces problèmes consiste à définir un ou plusieurs facteurs de rattachement qui, au mieux, permettraient d'identifier une législation applicable. Cette démarche est particulièrement délicate dans le cas des réseaux internationaux d'ordinateurs ou, en raison de la dissémination et du mouvement rapide des données et de la dispersion géographique des activités de traitement de l'information, plusieurs facteurs de rattachement pourraient intervenir de façon complexe en mettant en jeu des éléments nouveaux du point de vue juridique. En outre, on ne sait trop quelle valeur accorder actuellement aux règles qui, par application mécanique, déterminent la législation nationale spécifique devant être appliquée. Tout d'abord, l'opportunité d'une telle solution paraît dépendre de l'existence, de notions juridiques et de structures réglementaires analogues, ainsi que du caractère obligatoire des engagements pris par les pays d'observer certaines normes en matière de protection des données de caractère personnel. En l'absence de ces conditions, on pourrait s'efforcer de formuler des principes plus souples impliquant la recherche d'une « législation appropriée » et se rattachant à l'objectif visé qui est d'assurer une protection efficace de la vie privée et des libertés individuelles. Ainsi, dans un cas où plusieurs législations sont susceptibles d'être applicables, il a été suggéré qu'une solution pourrait consister à accorder la préférence à celle qui offre la meilleure protection des données de caractère personnel. En revanche, on peut faire valoir que des solutions de ce type laissent planer trop d'incertitude, en particulier du point de vue des maîtres de fichier qui pourront souhaiter connaître, s'il y a lieu à l'avance, à quel ensemble de règles nationales un système international de traitement de l'information sera soumis.

76. Compte tenu de ces difficultés et estimant qu'il pourrait y avoir intérêt à traiter les problèmes de conflits de loi dans le contexte global des données de caractère personnel et des données sans caractère personnel, le Groupe d'experts a décidé de se limiter à une déclaration qui consiste simplement à signaler les problèmes et à recommander aux pays Membres de s'employer à leur trouver une solution.

Activités ultérieures

77. Le Groupe d'experts appelle l'attention sur le libellé de la Recommandation 4 relative aux lignes directrices, laquelle suggère que les pays Membres conviennent dès que possible de procédures spécifiques de consultation et de coopération en vue de l'application des lignes directrices