Exposé des motifs

Recommandation No.R (91) 10 du Comité des Ministres aux Etats membres sur la communication à des tierces personnes de données à caractère personnel detenues par des organismes publics
(adoptée par le Comité des Ministres le 9 septembre 1991, lors de la 461e réunion des Délégués des Ministres)

Préambule - Les problèmes identifiés

1. L'"union plus étroite entre ses membres" objectif du Conseil de l'Europe - peut être atteinte au moyen de toute une gamme de possibilités. L'article 1 du Statut de l'Organisation se réfère expressément à la mission du Conseil de l'Europe pour le maintien et la promotion des droits de l'homme et des libertés fondamentales comme moyen de réaliser cette "union plus étroite".

2. La présente recommandation entre précisément dans cet objectif. Elle constitue un instrument des droits de l'homme. La recommandation vise la circulation de l'information au sein de la société et, parallèlement, la protection de la vie privée de l'individu. En d'autres termes, l'article 8 (le droit au respect de la vie privée), et l'article 10 (la liberté d'expression) de la Convention européenne des Droits de l'Homme sont des valeurs qui sous-tendent les différents principes contenus dans la recommandation.

3. Ces considérations de droits de l'homme expliquent les références faites dans le préambule à certains instruments juridiques essentiels adoptés par le Comité des Ministres du Conseil de l'Europe dans le domaine de l'information en général ainsi que dans celui de la protection de la vie privée: la Recommandation N° R (81) 19, la Déclaration du Comité des Ministres du 29 avril 1982, la Convention sur la protection des données du 28 janvier 1981. Tous ces instruments juridiques visent à promouvoir (et à concilier) les libertés fondamentales énoncées aux articles 8 et 10 de la Convention européenne des Droits de l'Homme.

4. Une politique visant la liberté d'information et une politique de protection de la vie privée peuvent chacune impliquer leur priorité propre. La promotion de chacune de ces valeurs fondamentales doit être fondée sur un respect mutuel. Parfois, il est nécessaire de concilier ces deux valeurs. Ceci explique, par exemple, le fait que la mise en oeuvre de la politique sur la liberté d'information contenue dans la Recommandation N° R (81) 19 est assujettie à la nécessité de respecter, entre autres, la vie privée de l'individu. Du point de vue de la protection de la vie privée, la mise en oeuvre d'une politique de protection des données doit, comme le précise le préambule de la Convention sur la protection des données, tenir compte de la nécessité de "... concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples". Pour le Comité intergouvernemental d'experts sur la protection des données, rédacteurs de cet instrument juridique, la politique de la liberté d'information et la protection des données ne constituent pas nécessairement des valeurs contradictoires. La protection des données devrait être conçue comme étant compatible avec les aspects plus larges d'une politique d'information au sein d'une société. La protection des données n'est pas destinée à imposer *a priori* des limitations à la circulation des informations à

caractère personnel dans la société. Ces principes visent, plutôt, à déterminer les conditions selon lesquelles les données à caractère personnel peuvent être collectées, traitées et communiquées à des tierces personnes, et utilisées par celles-ci.

5. Il convient de souligner d'emblée que le but de la présente recommandation n'est pas de promouvoir la transparence au sein de l'administration publique, ni d'encourager la liberté d'information. La Recommandation N° R (81) 19 du Comité des Ministres a déjà traité de l'opportunité de rendre les organismes publics responsables au moyen des principes de liberté d'information.

Le type de principes préconisés dans la Recommandation N° R (81) 19 est reflété dans nombre de systèmes juridiques nationaux. Il existe, par exemple, une législation générale sur l'accès à l'information du secteur public en Autriche, au Danemark, en Finlande, en France, en Grèce, aux Pays-Bas, en Norvège et en Suède. D'autres pays prévoient l'accès à certaines catégories d'information du secteur public. Les rédacteurs de ce texte s'intéressent essentiellement à la façon dont le principe de transparence (soit dans le contexte d'une législation générale, soit dans le contexte d'une législation sectorielle) s'articule avec la protection à accorder à la vie privée d'un individu dont les données à caractère personnel peuvent être communiquées à des tierces personnes qui demandent à y avoir accès. En outre, si des informations personnelles doivent être collectées, enregistrées et utilisées par des organismes publics conformément à la politique générale de protection des données et si, comme on l'a déjà noté (voir paragraphe 4), la politique de protection des données n'entrave pas *a priori* la communication des données à caractère personnel par des organismes publics à des tierces personnes en vertu d'une législation sur l'accès, comment déterminer les conditions de la communication?

6. En outre, une approche complète de la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel par des organismes publics à des tierces personnes ne peut se limiter uniquement à des situations prévues dans des dispositions régissant l'accès à l'information du secteur public. La recommandation aborde également tous les cas de figure dans lesquels les organismes publics collectent et enregistrent des catégories différentes de données à caractère personnel en vue de les rendre accessibles à des tierces personnes en vertu de toute une gamme de dispositions juridiques régissant l'accès. En particulier, la recommandation concerne les catégories de ce que l'on appelle des "fichiers publics" qui contiennent des données à caractère personnel publiées conformément à la loi. Ces fichiers, et le paragraphe 24 de ces commentaires en fournit des exemples, sont disponibles pour consultation par le public et les données qui y sont contenues peuvent être communiquées à des tierces personnes.

7. Les préoccupations de protection des données exprimées par les rédacteurs de cette recommandation s'inscrivent dans le contexte des nouvelles tendances apparues dans la gestion des fichiers de données à caractère personnel par des organismes publics. à savoir la communication électronique de données à caractère personnel ou de fichiers contenant des données à caractère personnel à des tierces personnes, ce qui a été rendu possible par le fait que l'informatique a permis aux organismes publics d'enregistrer les données qu'ils collectent dans des fichiers électroniques. En raison de la nature interventionniste et réglementaire des pouvoirs publics, la vie de tout citoyen s'en trouve par là-même affectée, et il n'est pas surprenant de constater que les bases de

données détenues par les organismes publics contiennent des quantités massives d'informations personnelles. Il n'est guère étonnant que la richesse de ces informations présente un grand intérêt pour des tierces personnes et, en particulier, les entreprises commerciales du secteur privé.

8. Comme le constate le préambule, il existe une tendance croissante de la part du secteur privé à exploiter des données à caractère personnel ou des fichiers contenant des données à caractère personnel en vue de servir des campagnes de marketing, de planifier une stratégie économique, de cibler une population de consommateurs éventuels, d'enrichir des fichiers de données à caractère personnel déjà existants, etc. C'est précisément l'automatisation des données à caractère personnel qui a favorisé leur exploitation par des tierces personnes. Les données peuvent faire l'objet d'un accès en ligne; les organismes publics peuvent aussi télédécharger eux-mêmes des catégories différentes de fichiers contenant des données à caractère personnel sur des bases de données de tierces personnes. Des sorties sur imprimante de noms et adresses sur des étiquettes sous forme automatisée peuvent être cédées par des organismes publics responsables de la gestion de différentes catégories de fichiers publics; ou bien, une tierce personne peut tout simplement acheter une bande magnétique de certains fichiers contenant des données à caractère personnel.

9. Il est intéressant de noter que la Commission des Communautés européennes a promulgué des lignes directrices destinées à améliorer la synergie entre secteur public et secteur privé sur le marché de l'information. Ces lignes directrices, adoptées en 1989, se réfèrent à l'abondance d'informations à la disposition des organismes publics et encouragent sa plus grande disponibilité dans le secteur privé:

"Les administrations collectent de manière régulière et systématique des données et des informations de base dans le cadre de leurs missions. Ces collections de données ont une valeur au-delà de leur utilisation par les administrations et un accès plus large à ces données serait bénéfique tant pour le secteur public que pour l'industrie." (Principe 1 des lignes directrices.)

10. La politique proposée peut, à l'évidence, facilement être analysée en termes de liberté d'information. Elle est tout à fait compatible par exemple avec l'article 10 de la Convention européenne des Droits de l'Homme qui ne se limite pas simplement à assurer la circulation de l'information pour la préservation et la promotion d'une société démocratique et pluraliste. La Déclaration du Comité des Ministres du 29 avril 1982 note, entre autres, que la liberté d'information et le droit pour toute personne de rechercher et de recevoir des informations sont nécessaires pour le développement social, économique, culturel et politique de tout être humain. Cela étant, comme il est déjà mentionné ci-dessus, il est essentiel d'intégrer dans cet ordre d'idées la politique de protection des données lorsqu'il s'agit d'informations à caractère personnel. Pour les rédacteurs de cette recommandation, ceci est encore plus crucial en raison des risques éventuels créés par la communication électronique de données à caractère personnel par des organismes publics et l'accès télématique de tierces personnes. à savoir l'établissement de profils électroniques de revenu individuel, de situation familiale, de titres de propriété, de l'état d'endettement, la quête de noms dans différents fichiers publics distincts, la mise en relation ou l'interconnexion des informations personnelles contenues dans de tels fichiers, ou bien l'utilisation des données pour des finalités qui n'ont pas motivé leur collecte et leur enregistrement

dans un fichier public, etc. En d'autres termes, les rédacteurs de la recommandation ont pris comme point de départ que le fait que des données à caractère personnel ou des fichiers contenant des données à caractère personnel soient accessibles à des tierces personnes conformément à des "dispositions juridiques" ne signifie pas nécessairement qu'ils ne doivent pas être protégés sous l'angle d'une politique de protection des données. Tel est, en fait, l'objectif premier de cette recommandation: comment déterminer les conditions dans lesquelles les données à caractère personnel peuvent être collectées et enregistrées dans de tels fichiers et, en particulier, les conditions dans lesquelles ces données à caractère personnel peuvent être communiquées à des tierces personnes et utilisées par celles-ci.

11. En analysant la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel par des organismes publics à des tierces personnes dans les deux situations décrites ci-dessus (conformément aux dispositions régissant l'accès à l'information du secteur public, ou en vertu de dispositions juridiques spécifiques concernant la publicité), les rédacteurs de la recommandation cherchent à souligner qu'un cadre juridique est essentiel avant que toute communication puisse être effectuée. En procédant ainsi, ils cherchent à éviter l'existence d'une zone grise ou une situation entre droit et non-droit, caractérisée par le fonctionnement de pratiques ou politiques administratives vagues. L'on peut noter en passant que le type d'action proposée dans la recommandation est compatible avec les conclusions émanant de la conférence organisée conjointement par le Conseil de l'Europe et la Commission des Communautés européennes (Luxembourg, 27-28 mars 1990) qui a examiné, entre autres, la question de l'accès à l'information du secteur public dans le nouvel environnement automatisé.

Dispositif - Type d'action qui pourrait être menée

12. Comme pour les recommandations antérieures qu'il a élaborées pour des secteurs particuliers, le Comité d'experts sur la protection des données offre une fois encore à l'intention des gouvernements un ensemble de principes de protection des données visant un nouveau contexte dans lequel l'informatique est intervenue et crée de nouveaux risques pour la vie privée de l'individu. Les principes contenus dans l'annexe à la recommandation peuvent à bien des égards être considérés comme s'ajoutant aux lignes directrices adoptées par la Commission des Communautés européennes pour améliorer la synergie entre secteur public et secteur privé sur le marché de l'information. Il convient de signaler que ces lignes directrices appellent l'attention des administrations publiques sur le besoin de protéger "les intérêts publics et privés légitimes" lors de la mise en oeuvre de la politique proposée dans celles-ci. En plus des informations auxquelles l'accès peut être restreint pour des raisons de sécurité nationale, de politique extérieure, ou de secret commercial, etc, les lignes directrices reconnaissent également que la protection de la vie privée et des données à caractère personnel constitue un motif légitime pour refuser de mettre à la disposition de tierces personnes des informations détenues par des organismes publics. Il est donc possible de considérer le corps des principes proposé par le Comité d'experts sur la protection des données comme un guide détaillé sur la manière par laquelle **les** Etats membres de la CEE (ainsi bien sûr que les Etats non membres) peuvent concrétiser ce besoin.

13. Le dispositif de la recommandation note également le rôle important des autorités nationales de protection des données dans l'application de ces principes. Certaines de ces autorités ont déjà manifesté leur volonté de limiter l'utilisation qui peut être faite par des organismes publics des données à caractère personnel qu'ils collectent dans des fichiers publics et auxquelles des tierces personnes peuvent avoir accès. En outre, la recommandation cherche également à associer les autorités établies en vertu de dispositions régissant l'accès à l'information du secteur public au schéma de protection avancé dans la recommandation. Comme il sera démontré à un stade ultérieur, une interpénétration du rôle de ces organes et des compétences des autorités de protection des données est encouragée en vue d'éviter une approche contradictoire de la communication par des organismes publics de données à caractère personnel ou de fichiers contenant des données à caractère personnel à des tierces personnes.

Annexe à la recommandation

1. Champ d'application et définitions

14. Comme on l'a noté dans le préambule, les principes contenus dans la recommandation visent la totalité des données à caractère personnel qui sont collectées par des organismes publics et qui peuvent être communiquées à des tierces personnes. Le texte du principe 1.1 passe sous silence toute référence à la nécessité que de telles données soient collectées par des organismes publics dans l'accomplissement de leurs fonctions officielles. Même s'il va sans dire que les organismes publics ne doivent collecter et enregistrer des données à caractère personnel qu'à des fins spécifiques et légitimes liées à leurs tâches autorisées, les rédacteurs de la recommandation estiment qu'il est bénéfique d'inclure dans son champ d'application toutes les données à caractère personnel collectées et détenues par des organismes publics qui peuvent être communiquées à des tierces personnes.

15. Le principe 1.1 souligne que la recommandation s'applique essentiellement aux données à caractère personnel traitées automatiquement par des organismes publics. Cette approche est conformé au souci principal qui a motivé cette recommandation, à savoir l'enregistrement électronique de données à caractère personnel et leur communication à des tierces personnes par des moyens télématiques. Néanmoins, comme on l'a noté au principe 1.2, les Etats membres peuvent étendre les principes de la recommandation aux données à caractère personnel qui sont détenues par des organismes publics et qui font l'objet d'un traitement manuel. Cette souplesse est importante étant donné que différentes catégories de données détenues par des organismes publics peuvent exister à la fois sous formes automatisée et manuelle. Par exemple, l'annuaire téléphonique - qui constitue un fichier de données à caractère personnel au sens de la recommandation - existe sous forme manuelle ainsi que sous forme électronique. L'on peut également noter en passant que la législation sur la protection des données d'un certain nombre d'Etats membres vise les deux formes de traitements.

16. Une liberté analogue visant à étendre le champ d'application de la recommandation s'applique aux données concernant les sociétés, les groupements, les

associations, etc, dotés ou non d'une personnalité juridique conformément au droit interne des sociétés. Bon nombre d'informations détenues par les organismes publics concernent de telles entités. Il suffit de se référer aux exemples fournis par les registres de sociétés *ou* les registres de commerce. Ceci est un facteur important à garder à l'esprit par les gouvernements des Etats membres dont la législation sur la protection des données couvre tant des personnes physiques que des personnes juridiques ainsi que tout autre organisme qui n'est pas doté d'une personnalité juridique.

17. L'on peut noter que les possibilités d'étendre le champ d'application de la recommandation mentionnées au principe 1.2 sont compatibles avec les dispositions de l'article 3, paragraphe 2.b et c de la Convention N° 108.

18. Le principe 1.3 est consacré à la définition de certaines expressions clés qui apparaissent fréquemment dans la recommandation.

19. La définition des "données à caractère personnel" mentionnée au principe 1.3 ne devrait pas soulever trop de problèmes étant donné que la formule a été acceptée par tous les Etats membres dans les recommandations sectorielles antérieures du Comité des Ministres dans le domaine de la protection des données. Les gouvernements devraient prêter une attention particulière à la question des données statistiques qui, même si elles ne sont pas détenues sous forme nominative, peuvent être néanmoins désanonymisées par le biais de techniques sophistiquées de traitement de données. Les rédacteurs de la recommandation ont noté que le Comité d'experts sur la protection des données a récemment entrepris une étude dans le domaine des données statistiques et l'on attend qu'un instrument juridique séparé soit élaboré en vue d'aborder les nouveaux problèmes posés par l'utilisation, y compris la communication, de données statistiques détenues par des organismes publics.

20. Les données à caractère personnel peuvent, bien évidemment, être mises en circulation et donc à la disposition du public, par des organismes des secteurs public et privé. Par exemple, les commerçants peuvent publier des registres publics contenant le nom et l'adresse de leurs membres. De même, des organismes professionnels du secteur privé peuvent faire paraître des annuaires contenant divers types d'informations personnelles sur leurs membres - le nom, l'adresse, les qualifications professionnelles, leurs domaines spécialisés, etc. Cela étant, la recommandation ne traite que des données à caractère personnel détenues par des "organismes publics". De tels organismes exercent des activités de service public ou d'intérêt public. On peut les trouver au niveau de l'Etat ou des collectivités locales. Contrairement aux organismes privés, les organismes publics sont soumis aux principes du droit public, y compris la possibilité de demander le contrôle juridictionnel de leurs actes administratifs. Bien entendu, la frontière entre les activités des organismes privés et celles des organismes publics a parfois des contours imprécis. Par exemple, il se peut que certains organismes, dépendant du point de vue budgétaire de l'Etat ou des collectivités locales, soient en concurrence sur le marché avec des entreprises privées et dans les mêmes conditions que des entreprises privées. En outre, des organismes privés peuvent dans certains pays effectuer des activités de service public ou d'intérêt public. L'on peut prendre comme exemple à cet égard des entreprises privatisées qui étaient auparavant juridiquement et économiquement situées dans le secteur public.

21. Tout en constatant qu'il est possible de dégager certains critères communs à tous les Etats en ce qui concerne les organismes publics, le texte admet que le droit interne peut avoir un point de vue plus large sur le type d'organismes qu'il peut qualifier de "publics" aux fins de la recommandation.

22. Le principe 1.1, comme noté précédemment, se limite aux données à caractère personnel qui sont collectées par des organismes publics et "pouvant faire l'objet d'une communication à des tierces personnes". La recommandation se fonde sur la nécessité d'une base juridique pour communiquer de telles données. Très souvent, de telles données sont contenues dans des "fichiers". Les données ne devraient être communiquées à des tierces personnes que si ces fichiers sont en fait "accessibles à des tierces personnes".

Le principe 1.3, 4e alinéa, identifie les différentes hypothèses dans lesquelles des tierces personnes peuvent avoir accès à des fichiers contenant des données à caractère personnel et en obtiennent communication. En premier lieu, les fichiers peuvent être accessibles à des tierces personnes conformément aux dispositions régissant l'accès à l'information relevant du secteur public ou la liberté d'information. Ces dispositions peuvent être trouvées dans des lois générales régissant la liberté d'information ou l'accès à l'information relevant du secteur public. Alternativement, de telles dispositions peuvent être trouvées dans des contextes juridiques plus limités. Dans certains pays, une législation générale coexiste avec des dispositions sectorielles d'accès. D'autres pays ne disposent que de règles sectorielles sur l'accès. Comme il a déjà été précisé, il n'est pas dans l'intention des rédacteurs de proposer des principes généraux visant l'accès à l'information du secteur public ou la liberté d'information, ni de modifier la législation et la procédure nationales pour l'octroi de l'accès, ni d'harmoniser le champ d'application d'une telle législation. Le Comité des Ministres a déjà encouragé cette action dans sa Recommandation N° R (81)19. La présente recommandation ne concerne que la nouvelle situation créée depuis l'automatisation des bases de données du secteur public et les possibilités ainsi offertes à des tierces personnes d'avoir accès plus facilement aux données nominatives contenues dans ces bases de données, sans avoir à justifier les raisons pour lesquelles les fichiers de données à caractère personnel sont demandés.

23. En outre, des fichiers peuvent être accessibles à des tierces personnes y compris au public en général parce que telle était l'intention du législateur dans des dispositions spécifiques. Ces catégories de fichiers visent les "fichiers publics" proprement dits qui contiennent des données à caractère personnel collectées et enregistrées par des organismes publics en vue de leur publication officielle. Bien que de tels fichiers soient généralement accessibles, il se peut que l'accès en soit limité à des groupes bien définis - par exemple, certains Etats limitent l'accès au casier judiciaire aux personnes travaillant dans le système pénal. Ce "groupe limité d'usagers" explique la référence faite au principe 1.3, 4e alinéa, "à des tierces personnes ayant un intérêt particulier".

24. Ces "fichiers publics" peuvent comprendre notamment les annuaires téléphoniques, les registres électoraux, les cadastres, les fichiers contenant le nom et l'adresse des consommateurs d'électricité et de gaz, les registres de brevets et de marques, les fichiers contenant des informations relatives à la tutelle, les registres de commerce, les registres d'immatriculation des véhicules, les registres établis par les

autorités de protection de données contenant des informations sur les utilisateurs de données, etc. La recommandation part du principe que de tels fichiers publics ont été créés en vertu de dispositions juridiques spécifiques. Ces dispositions juridiques spécifiques peuvent être des lois, des règlements, des décrets-lois, etc: Ce qui est important, c'est que la publication des informations et leur accessibilité au public, y compris à des tierces personnes, soient prévues par la loi, et dans le cas de certains pays, conformément aux dispositions régissant l'accès à l'information du secteur public, et plus communément, conformément aux dispositions juridiques spécifiques régissant les fichiers publics.

25. Il existe de nombreuses raisons pour lesquelles de tels fichiers publics peuvent voir le jour. Par exemple, ils peuvent être créés dans le cadre d'une loi en vue de favoriser les impératifs de transparence dans une certaine activité économique, le cas typique étant celui de la publication du nom des dirigeants de sociétés. Les informations peuvent aussi être rendues publiques en vue de promouvoir l'intérêt public dans différents domaines, par exemple pour rendre accessibles au public le nom et l'adresse des personnes ayant droit de vote lors d'élections nationales ou locales. Des informations peuvent encore être rendues publiques afin de faciliter les relations entre les individus, l'exemple type étant celui des annuaires téléphoniques. Enfin, la nature interventionniste des pouvoirs publics conduit à une réglementation accrue de différentes activités. Qui dit réglementation dit contrôle qui s'exerce sur les participants à ces activités - par exemple, par le biais de procédures de délivrance d'autorisations. Il n'est pas rare de trouver des listes de titulaires d'autorisation (usagers de données, détenteurs de permis de port d'arme à feu, permis de pêche, etc) publiées en vertu d'un texte de loi, et donc à la disposition du public.

26. Le terme "communication", qui apparaît dans le titre même de la recommandation, est défini d'une manière large. La définition couvre tant la communication massive que la communication non massive de données à caractère personnel contenues dans des fichiers accessibles à des tierces personnes. La définition est rédigée de façon à être technologiquement à jour. Elle vise la communication par des moyens électroniques ou télématiques, la consultation électronique par des méthodes en ligne ainsi que la délivrance de bandes magnétiques et le télédéchargement de données à caractère personnel ou de fichiers contenant des données à caractère personnel.

27. Les "tierces personnes" sont définies afin d'exclure spécifiquement la communication à des organismes publics. La définition vise clairement des compagnies, des groupes et des associations relevant du secteur privé, ainsi que des individus. Les rédacteurs de la recommandation n'ont pas traité la question de la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel entre des organismes publics soit à des fins d'intérêt public liées à leurs fonctions officielles soit à d'autres fins telles que le marketing ou la stratégie économique en dehors du cadre strict de leurs fonctions. A l'instar des questions statistiques évoquées au paragraphe 19, les rédacteurs de la recommandation ont noté que le Comité d'experts sur la protection des données pourrait porter une attention particulière à la communication de données à caractère personnel entre organismes publics dans le cadre d'un instrument juridique séparé.

28. Néanmoins, comme on l'a noté au cours de la discussion, dans la définition des "organismes publics" une zone d'ombre peut exister entre les activités d'organismes

publics et d'organismes privés, et les différents Etats peuvent percevoir de manière différente les notions d'organisme privé et d'organisme public. Les approches différentes éventuelles de ce problème expliquent la raison pour laquelle la recommandation introduit une certaine souplesse quant au champ d'application de l'expression "tierces personnes", permettant ainsi aux Etats d'élargir la portée de cette expression (principe 1.3, alinéa 7).

2. Respect de la vie privée et principes de protection des données

29. Les principes contenus dans la recommandation sont destinés bien sûr à assurer le droit au respect de la vie privée de la personne concernée lorsque ses données sont communiquées par des organismes publics à des tierces personnes. Le cadre protecteur donc, proposé dans le corps de la recommandation, est conforme aux garanties du respect de la vie privée énoncées à l'article 8 de la Convention européenne des Droits de l'Homme. Les rédacteurs de la recommandation ont également pris comme point de départ le fait que le droit au respect de la vie privée devrait être renforcé en se référant aux principes de protection des données qui réglementent les conditions dans lesquelles les données à caractère personnel peuvent être communiquées et, en particulier, le rôle précis de la personne concernée dans la détermination de ces conditions. Autrement dit, la recommandation est plus axée sur le respect de la vie privée dans le sens de l'autodétermination informationnelle que sur le "droit d'être laissé seul". Cette approche de la protection de la vie privée est mieux adaptée aux nouvelles réalités technologiques caractérisant la politique des organismes publics à l'égard des données à caractère personnel qu'ils détiennent ainsi qu'aux nouvelles menaces pour la vie privée de l'individu, son autonomie, sa dignité et son identité engendrées par le mauvais usage des données à caractère personnel par des moyens techniques lorsque les données ont été communiquées à des tierces personnes.

30. Gardant ces facteurs à l'esprit, le principe 2 de la recommandation se réfère à la nécessité de prévoir des sauvegardes et des garanties accompagnant la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel à des tierces personnes. Le principe 2.1 souligne que la communication de données à caractère personnel doit reposer sur un fondement juridique autorisant une telle communication. A titre d'illustration, le principe se réfère à des lois spécifiques, par exemple les lois régissant différents types de fichiers publics; à des dispositions sur la liberté d'information qui peuvent être de nature générale ou sectorielle; à une autorisation fournie conformément à une législation sur la protection des données, y compris par exemple l'autorisation d'une autorité établie dans le cadre d'une telle législation. Toutes ces différentes sources juridiques peuvent constituer le fondement d'une communication.

En l'absence d'un tel fondement juridique, le principe 2.1.*d* précise que la communication doit dépendre de l'obtention du "consentement exprès et éclairé" de la personne concernée.

31. Le principe 2.2 met en lumière l'importance de continuer à respecter le principe du but spécifique ou de la finalité après le stade de la communication. Les données à caractère personnel collectées par les organismes publics devront avoir été collectées à des fins déterminées et légitimes liées à leurs fonctions officielles. Conformément à

l'article 5.b de la Convention N° 108, les données ainsi collectées ne devraient pas être utilisées, y compris communiquées, pour d'autres finalités incompatibles. Le principe 2.2 tend à concrétiser le principe du but spécifique ou de la finalité dans le secteur couvert par la recommandation. Ayant cet objectif à l'esprit, le principe 2.2 prévoit que les données à caractère personnel ou les fichiers contenant des données à caractère personnel ne peuvent pas être communiqués à des tierces personnes pour des finalités incompatibles avec celles pour lesquelles les données ont été collectées, à moins qu'il n'existe en droit interne des sauvegardes et garanties appropriées. Au paragraphe 33 ci-dessous, il est expliqué ce qu'il convient d'entendre par "des sauvegardes et garanties appropriées". S'agissant de l'expression "droit interne", il convient de retenir une interprétation large. Cela peut aller de l'autorisation comprise dans un statut de création d'un fichier public particulier à une décision prise par une autorité de protection des données, ou par une agence établie en vertu de la législation sur la liberté d'information.

32. Il est admis dans de nombreuses lois régissant l'accès aux informations du secteur public (l'un des mécanismes juridiques permettant à des tierces personnes d'accéder à des fichiers contenant des données à caractère personnel) que la tierce personne demanderesse n'est pas tenue de justifier les raisons pour lesquelles elle souhaite avoir accès aux données ou aux fichiers contenant des données, ni les finalités pour lesquelles elle les utilisera. La Recommandation N° R (91) 19 du Comité des Ministres exprime le même principe de non-justification d'une demande d'accès. En conséquence, dans de nombreux pays où il existe des lois générales sur la liberté de l'information ou sur l'accès aux informations du secteur public, les organismes publics ne peuvent pas restreindre la communication de données à caractère personnel au motif que les données recherchées seront utilisées pour des fins incompatibles. Cela dit, certains pays en Europe envisageaient - au moment de la rédaction de cet exposé des motifs - de restreindre l'utilisation de l'accès aux informations du secteur public pour des finalités d'exploitation commerciale. Les rédacteurs de la recommandation pensent que les nouvelles tendances visant à enregistrer des données à caractère personnel ou des fichiers contenant des données à caractère personnel sous forme électronique permettant ainsi une communication télématique, y compris sous forme massive, conformément aux dispositions régissant l'accès aux informations du secteur public, exigent que tous les Etats procèdent à une révision des utilisations qui sont faites de ces lois. Il est possible que ces nouveaux développements n'aient pas été présents dans l'esprit des rédacteurs de ces lois lorsqu'ils ont cherché à promouvoir une transparence au sein des administrations publiques et la responsabilité des autorités publiques.

33. Concernant le type de sauvegardes et de garanties qui pourraient être prises, il est fait référence à des questions telles que la nécessité de recueillir le consentement exprès et éclairé de la personne concernée avant que les données ne soient communiquées pour des finalités incompatibles, ou au moins de les informer lors de la collecte des données que celles-ci peuvent être communiquées à des tierces personnes pour des finalités autres que celles qui ont motivé leur collecte: ce qui leur donnerait la possibilité de soulever une objection. Ces points sont traités de manière détaillée aux principes 4 et suivants.

34. Le principe 2.3 contient une déclaration générale sur le fait que le traitement des données par des tierces personnes après leur communication est assujetti aux

exigences de la législation interne (notification, déclaration, enregistrement de fichiers contenant des données à caractère personnel, etc) sur la protection des données, y compris aux contrôles de procédure exercés par les autorités chargées de la protection des données. Le principe 6 donne plus de détails sur la manière dont les données peuvent être utilisées par les tierces personnes auxquelles elles ont été communiquées. Toutefois, le principe 2.3 est tout à fait clair en indiquant que la législation sur la protection des données couvre l'utilisation ainsi que d'autres étapes du traitement, telles que la conservation des données.

3. Données sensibles

35. Les rédacteurs de la recommandation ont structuré leur approche de la question de la communication des données en fonction de la nature des données collectées par les organismes publics. La nature des données détermine leur accessibilité à des tierces personnes et, par conséquent, les conditions de leur communication. Cette approche est reflétée dans les dispositions du principe 3 de la recommandation ainsi que dans les principes 4 et suivants de la recommandation. Le principe 3 concerne les données à caractère personnel généralement non accessibles à des tierces personnes en raison de leur sensibilité ou du risque de préjudice à la vie privée des personnes concernées si elles étaient communiquées à des tierces personnes. Les principes 4 et suivants, par ailleurs, concernent les données à caractère personnel qui sont généralement accessibles conformément à des dispositions juridiques. La nature de telles données est différente et au lieu de bloquer ou de suivre une approche extrêmement restrictive quant à leur communication, comme c'est le cas pour les catégories de données visées au principe 3, il s'agit plutôt de déterminer les conditions dans lesquelles ces données peuvent être communiquées.

36. Le principe 3.1 considère comme "données sensibles" toutes les catégories de données sensibles mentionnées à l'article 6 de la Convention N° 108 (les données révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, les données personnelles de santé, les données relatives à la vie sexuelle ou les données concernant les condamnations pénales). Il conviendrait de garder à l'esprit que l'article 6 ne constitue pas une liste exhaustive de telles données. Les Etats membres peuvent avoir d'autres conceptions de la notion de données sensibles.

37. La règle générale relative aux données sensibles est clairement énoncée au principe 3.1**,** à savoir que de telles données ne devraient pas être enregistrées dans un fichier généralement accessible à des tierces personnes. Les rédacteurs de la recommandation ont reconnu qu'une telle règle générale ne pouvait pas avoir une nature absolue. Par exemple, dans certains pays des listes de jugements de faillite prononcés contre certaines personnes peuvent être à la disposition du public pour consultation. Etant donné que certains de ces pays peuvent considérer les jugements de faillite comme étant des condamnations pénales, la liste qui est rendue accessible aux tierces personnes contiendra l'une des catégories sensibles mentionnées à l'article 6 de la a)De plus, la nécessité de contrôler le recrutement par les entreprises de personnes appartenant à des minorités ethniques ou religieuses peut conduire à créer des fichiers accessibles aux tierces personnes contenant des données sensibles Toutefois, étant donné le caractère fondamental des sauvegardes prévues au principe 3.1, toute exception à ce principe peut seulement être acceptée dans des circonstances bien définies prévues par la loi et accompagnées de sauvegardes et garanties

équivalentes. Tel est l'objectif de la clause du second alinéa du principe 3.1. En rédigeant cette clause, les rédacteurs de la recommandation se sont fondés sur les dérogations pertinentes contenues à l'article 9 de la Convention N° 108. Par exemple, les deux exceptions visées précédemment peuvent être fondées sur les dispositions de l'article 9 qui se réfère à "la répression des infractions pénales" ainsi qu'à "la protection des droits et libertés d'autrui". S'agissant des "garanties et sauvegardes appropriées" mentionnées au second alinéa du principe 3.1, les rédacteurs ont songé aux catégories de garanties visées à l'article 6 de la Convention N° 108.

38. La référence à "enregistrées dans un fichier ou dans la partie d'un fichier" est justifiée en raison du fait que certains fichiers, pouvant être généralement accessibles, peuvent contenir également des données à caractère personnel de nature sensible. Le cadre protecteur proposé dans le principe 3.1 serait gravement affaibli si le texte ne réglementait pas cette éventuelle lacune.

39. Le principe 3.2 traite des situations dans lesquelles des organismes publics détiennent des listes de noms d'hommes politiques et leur appartenance politique ou des listes de noms de personnes qui, bien que ne faisant pas partie de la classe politique, sont néanmoins impliquées dans la vie politique. Par exemple, ces personnes peuvent avoir été nommées aux cabinets de ministres sur la base de leur affiliation politique. Bien entendu, cette catégorie de données est *a priori* sensible puisqu'elle tombe dans l'une des catégories énoncées à l'article 6 de la Convention N° 108.

40. D'autres situations n'impliquant pas des données concernant des opinions politiques peuvent également être envisagées. Par exemple, les organismes publics peuvent détenir des listes de noms de personnalités religieuses indiquant leur affiliation religieuse spécifique. Une fois encore, ces données relèvent *a priori* de l'article 6 de la Convention N° 108 puisqu'elles ont trait à des convictions religieuses.

41. Néanmoins, les rédacteurs de la recommandation ont estimé que dans ces circonstances, ces données *a priori* sensibles pouvaient être rendues accessibles à des tierces personnes, puisque les données en question relèvent du "domaine public".

42. Les rédacteurs de la recommandation sont arrivés à cette conclusion sur la base d'une interprétation de l'article 6 de la Convention N° 108. De leur point de vue, les données relatives à des personnes impliquées dans la vie publique ne "révèlent" pas, au sens strict du terme, des sujets tels qu'opinions politiques ou convictions religieuses. De plus, les rédacteurs de la recommandation pensent que le fait de rendre accessibles à des tierces personnes des données relevant du domaine public est également justifié par l'article 9, paragraphe 2.b de la Convention N° 108. L'on estime que l'accessibilité des données est justifiée puisqu'elle contribue à la transparence et, en tant que telle, est destinée à la protection "des droits et libertés d'autrui".

43. En outre, lors de l'élaboration de cette disposition, les rédacteurs ont tenu compte de l'arrêt de la Cour européenne des Droits de l'Homme dans l'affaire Lingensxx; dans cette affaire, la Cour a indiqué que contrairement à un simple particulier, un homme politique "... s'expose inévitablement et consciemment à un contrôle attentif

de ses faits et gestes tant par les journalistes que par la masse des citoyens ...". On a estimé qu'un raisonnement similaire pouvait être appliqué à toute personne concernée par la vie publique.

44. Le principe 3 ne traite pas des données à caractère personnel qui, bien que n'étant pas sensibles stricto sensu, pourraient néanmoins porter préjudice à la vie privée des personnes concernées si elles étaient généralement accessibles. Par exemple, des données détenues par des organismes publics concernant des facteurs humains tels que la tutelle, l'adoption ou le divorce dans les registres civils pourraient être une cause de détresse pour des personnes si ces données étaient généralement accessibles. L'on estime que les Etats membres devraient élaborer des politiques spécifiques pour la communication de telles données en vue d'éviter qu'un préjudice ne soit causé à la vie privée des personnes concernées. Par exemple, on devrait tenir compte de la possibilité de ne communiquer de telles données qu'à des tierces personnes ayant un intérêt légitime à les obtenir ou d'empêcher ou de restreindre une délivrance massive des fichiers dans lesquels les données sont enregistrées.

Il peut naturellement arriver que des noms contenus dans des fichiers accessibles à des tierces personnes révèlent des données sensibles telles que l'origine ethnique ou la religion. Ce point n'est pas traité dans la recommandation. On a estimé qu'il s'agit là d'une conséquence inévitable de l'inclusion de noms dans un fichier public. Toutefois, il convient de se référer aux dispositions des principes 5.2 et 7 qui visent à réglementer les circonstances dans lesquelles des noms peuvent être extraits de fichiers accessibles à des tierces personnes.

4. Données généralement accessibles

45. Le principe 4 fournit des lignes spécifiques sur la manière dont "les données généralement accessibles", devraient être collectées par les organismes publics. Le principe 4, on le verra, est lié aux dispositions du principe 6 étant donné que les circonstances dans lesquelles la collecte des données se fera influenceront les conditions dans lesquelles elles pourront ultérieurement être communiquées à des tierces personnes.

46. Les principes 4.1 et 4.2 doivent être considérés comme des principes de base d'une transparence au stade de la collecte des données. En outre, ils reflètent la nécessité d'assurer qu'une personne ne doit pas simplement être considérée comme une source riche et inconsciente de données à caractère personnel. La personne concernée doit être intégrée dans le circuit de l'information. De plus, le principe 4.1 souligne le fait que les fichiers qui doivent être rendus accessibles à des tierces personnes n'est pas une question neutre de protection des données. Une fois encore, la nécessité d'un cadre juridique régissant la communication de données à caractère personnel à des tierces personnes est mise en exergue.

47. Toutes ces sauvegardes et garanties contribuent à l'élaboration d'une politique de protection des données pour des données à caractère personnel ou des fichiers contenant des données à caractère personnel accessibles à des tierces personnes. Comme les autres principes de la recommandation, elles sont destinées à assurer que le nouveau marché de l'information qui s'établit et qui est particulièrement encouragé par les lignes directrices de la Commission de la CEE dont il a été fait mention plus

haut n’ignore pas le fait que des informations personnelles ne doivent pas être simplement perçues en termes de ressource économique. Il doit aussi être vu sous l’angle des droits de l’homme et des libertés fondamentales, en particulier du droit à la protection des données.

48. Ayant ces facteurs à l’esprit, il a été recommandé au principe 4.1 que les finalités pour lesquelles les données seront collectées et traitées dans des fichiers accessibles à des tierces personnes ainsi que l’intérêt public justifiant leur accessibilité soient indiqués conformément au droit et à la pratique internes. Les facteurs mentionnés au principe 4.1 peuvent être indiqués soit expressément soit implicitement et pas nécessairement par la loi. La référence à la "pratique" permet aux Etats membres d’utiliser des méthodes telles que les médias ou les formulaires. officiels ou d’autres mécanismes appropriés pour indiquer les finalités pour lesquelles les données seront collectées et traitées dans des fichiers accessibles à des tierces personnes ainsi que l’intérêt public justifiant leur accessibilité. Il suffit, par exemple, qu’il existe une loi sur l’accès à l’information du secteur public ou sur la liberté d’information dans un pays donné autorisant l’accès général aux données à caractère personnel détenues par des organismes publics. En outre, l’intérêt public justifiant l’accessibilité peut se trouver dans la nature d’une telle législation générale - la nécessité de promouvoir une transparence et une responsabilité au sein des administrations publiques. En ce qui concerne les catégories de "fichiers publics", au sens classique du terme, des statuts spécifiques régissent très souvent les finalités pour lesquelles ils peuvent exister ainsi que les raisons motivant ces finalités.

49. Comme pour le principe 4.1, le principe 4.2 se réfère au droit et à la pratique internes comme constituant l’instrument approprié pour faire savoir aux personnes concernées si elles sont juridiquement tenues ou non de fournir leurs données à un organisme public et ce, avant la collecte ou au moment de celle-ci. Le paragraphe 48 ci-dessus indique ce qu’il faut entendre par droit et pratique internes. Dans le cas d’un recensement ou d’un registre électoral, la personne devrait être informée qu’elle est obligée, de par la loi, de fournir certains détails personnels. Alternativement, dans le cas d’un annuaire téléphonique, la personne concernée devrait être informée qu’il n’existe aucune contrainte juridique visant à ce que ses données soient enregistrées dans un fichier accessible à des tierces personnes. De plus, les personnes concernées devraient être informées des fondements juridiques de la collecte ainsi que des finalités pour lesquelles les données sont enregistrées et traitées. Enfin, les personnes concernées devraient être informées de l’intérêt public qui justifie le fait que leurs données seront accessibles à des tierces personnes.

50. Le principe 4.3 encourage les organismes publics à être sensibilisés aux besoins des personnes concernées dont la sécurité et la vie privée pourraient être particulièrement menacées si leurs données étaient accessibles au public en général. Par exemple, les organismes publics devraient tenir compte des demandes de personnes travaillant dans des services de sécurité ou qui ont d’autres raisons légitimes d’échapper à la publicité de ne pas souhaiter que leurs données soient livrées au public.

5. Accès et communication de données à caractère personnel par le biais de moyens électroniques

51. Le principe 5 de la recommandation met en avant un certain nombre de sauvegardes et de garanties pour les données à caractère personnel qui sont traitées automatiquement et qui sont contenues dans des fichiers accessibles à des tierces personnes. En premier lieu, les opérations de traitement effectuées par les organismes publics sont assujetties aux dispositions du droit interne. Ces dispositions, qui peuvent prendre la forme de réglementations spécifiques pour les divers types de bases de données électroniques détenues par les organismes publics, devraient déterminer la manière dont les données à caractère personnel peuvent être communiquées et rendues accessibles à des tierces personnes. En particulier, l'utilisation de moyens techniques pour communiquer ou consulter des fichiers électroniques devrait être encadrée juridiquement. Il existe des moyens pratiques de le faire. Par exemple, chaque fois que les organismes publics rendent leurs fichiers publics accessibles en ligne, ils devraient conclure un contrat avec les tierces personnes qui souhaitent procéder à un déchargement télématique des fichiers contenant des données à caractère personnel dans leurs propres bases de données. Ce contrat pourrait contenir des clauses qui refléteraient toutes les conditions et limites régissant les recherches dans les fichiers contenant des données à caractère personnel. En outre, le contrat pourrait obliger la tierce personne à respecter toutes les conditions imposées par la personne concernée pour l'utilisation ultérieure des données. De plus, le contrat pourrait servir de moyen pour avertir la tierce personne de la nécessité d'utiliser les données à caractère personnel conformément au droit interne et à la procédure sur la protection des données.

52. Les dispositions du principe 5.2 sont destinées à aborder la question de la sécurité des fichiers électroniques susceptibles d'accès ou de consultation en ligne. Des mesures techniques devraient être prises afin d'empêcher un télédéchargement en masse de fichiers contenant des données à caractère personnel en infraction avec les réglementations régissant la tenue et la communication de fichiers électroniques. De plus, l'on devrait tenir compte de la nécessité éventuelle de limiter les critères de base selon lesquels les données à caractère personnel peuvent être recherchées. Ce point est discuté plus loin dans les commentaires relatifs au principe 6.3.

6. Traitement par des tierces personnes de données à caractère personnel provenant de fichiers accessibles à des tierces personnes

53. i. Situation dans laquelle la personne concernée est tenue juridiquement de fournir ses données (principe 6.1)

Il y a lieu de souligner que les termes "juridiquement tenue" ne visent pas seulement les cas d'obligation de fournir les données résultant d'une loi (par exemple, en vertu d'obligations fiscales ou en cas de recensement), mais couvrent également les situations dans lesquelles les personnes concernées doivent fournir des données pour recevoir divers avantages ou services sociaux (par exemple, éducation, sécurité sociale ou même la bénédiction de l'Etat pour se marier).

ii. Situation dans laquelle la personne concernée fournit de manière volontaire ses données à un organisme public (principe 6.2)

La personne concernée peut par exemple avoir répondu à un questionnaire envoyé par une autorité locale, les réponses étant destinées à aider cette autorité locale à établir les besoins de la population concernée.

54. Etant donné que la personne concernée n'a pas eu la possibilité de refuser la collecte et l'inclusion ultérieure de ses données dans des fichiers accessibles à des tierces personnes, parce qu'elle était juridiquement tenue de fournir les données, les principes 6.1 et 6.2 donnent à la personne concernée des garanties compensatoires de manière à réglementer le traitement ultérieur de ses données par des tierces personnes. C'est dans cette optique que le principe 6.1 exige que le consentement exprès et éclairé de la personne concernée - et ce consentement devrait être révocable en tout temps - soit recueilli avant que les tierces personnes ne puissent réutiliser les données. Pour que ce principe du consentement exprès et éclairé soit significatif, on devrait bien entendu demander à la personne, lors de la collecte, si elle consent ou non à ce que ses données à caractère personnel soient communiquées à des tierces personnes par l'organisme public responsable de la collecte et de l'accessibilité. En l'absence du consentement exprès et éclairé de la personne concernée, le traitement de données à caractère personnel par des tierces personnes ne devrait pouvoir être effectué qu'en conformité avec les prescriptions de textes législatifs. De telles exigences ou prescriptions législatives pourraient être incluses dans les lois régissant des catégories spécifiques de fichiers publics, les législations sur la protection des données ou sur la liberté d'information.

55. Lorsque la personne concernée n'a pas été obligée de fournir ses données dans les conditions indiquées ci-dessus, elle devrait avoir la possibilité d'exercer certains droits à l'égard de ses données enregistrées dans un fichier accessible à des tierces personnes. Les droits énoncés au principe 6.2.a, b, c et d ne doivent pas nécessairement être tous reflétés dans le droit interne. Il résulte clairement du principe 6.2 qu'il s'agit d'options dont l'une au moins devrait être prévue par le droit interne.

56. Le principe 6.3 souligne les droits liés à la protection des données de la personne concernée à l'égard de ses données traitées par des tierces personnes et obtenues à partir de fichiers accessibles à des tierces personnes. Ces droits comprennent le droit d'accès, de rectification et d'effacement lorsque les données ont été traitées en violation des principes de protection des données. Les droits énoncés au principe 6.3 sont un simple énoncé du contenu de l'article 8 de la Convention sur la protection des données. Cependant, le deuxième alinéa du principe 6.3 se réfère en particulier au droit de la personne concernée de faire effacer ses données des nouveaux fichiers créés par des tierces personnes sur la base de données accessibles à des tierces personnes. Bien que le droit d'effacement prévu à l'article 8 de la Convention sur la protection des données dépende du fait que les données aient été traitées de manière irrégulière, les rédacteurs de la recommandation ont estimé, néanmoins, qu'il était approprié d'octroyer un droit à l'oubli sans restriction dans les situations couvertes par la recommandation. Il convient de noter que l'approche suivie par les rédacteurs en matière de droit d'effacement est compatible avec l'approche précédente suivie dans la Recommandation N° R (85) 20 sur la protection des données à caractère personnel utilisées à des fins de marketing direct. Il conviendrait de se référer à cette recommandation pour les principes supplémentaires régissant la manière dont les données à caractère personnel couvertes par la présente recommandation peuvent être réutilisées par des tierces personnes à des fins de marketing.

7. Appariement-mise en relation de fichiers

57. Les principes contenus dans la présente recommandation sont destinés à être technologiquement pertinents. Comme cela a été mentionné à différents stades du texte, les principales préoccupations visent à éviter des abus possibles résultant de l'introduction et de l'utilisation de la technologie de traitement des données par les organismes publics et des nouveaux moyens électroniques de communication des données qu'ils détiennent.

57. La technologie de traitement des données est aussi à la disposition des tierces personnes auxquelles les données peuvent être communiquées. A l'aide de programmes de logiciels, elles peuvent électroniquement balayer des fichiers publics pour isoler des noms et adresses sur la base de certains critères - par exemple, l'âge ou l'origine raciale. Des tierces personnes peuvent actuellement produire des nouveaux fichiers plus intéressants à partir d'informations contenues dans divers fichiers isolés détenus par des organismes publics. Les nouveaux fichiers résultant de ce procédé peuvent être extrêmement riches en termes de données à caractère personnel, et certainement plus complets en informations qu'un fichier pris séparément. Il est, par exemple, possible d'interconnecter l'annuaire téléphonique avec une autre catégorie de fichier public afin d'augmenter la valeur des informations contenues dans l'annuaire téléphonique électronique.

58. Ces nouvelles techniques d'appariement ou de mise en relation de fichiers présentent de véritables dangers. Ils peuvent notamment fournir des profils automatiques de style de vie sur des personnes à leur insu et sans leur consentement. En outre, la possibilité d'isoler des noms à partir de fichiers publics sur la base d'une nationalité ou d'une religion que laissent supposer les noms permet de créer des fichiers contenant des données sensibles. C'est pour cette raison que le principe 5.2 de la recommandation propose de limiter le champ des interrogations électroniques ou des recherches électroniques des fichiers accessibles au public. Par exemple, l'on devrait tenir compte de la nécessité d'empêcher des recherches électroniques dans des fichiers publics limités à des noms particuliers de personnes vivant dans des régions ou des localités spécifiques. Le télédéchargement de telles informations, associé à la possibilité de les apparier ou de les interconnecter avec un autre fichier, pourrait permettre à des tierces personnes d'obtenir des données sensibles très précises sur des groupes bien définis.

59. Conscients des problèmes évoqués au paragraphe précédent, les rédacteurs de la recommandation ont recommandé que les techniques d'appariement ou de mise en relation de fichiers ne devraient être permises que par le droit interne. De plus, le droit interne - qui devrait une fois encore être interprété de manière large - devrait prévoir des sauvegardes appropriées pour la personne concernée dans le cas où une autorisation serait donnée à des tierces personnes d'utiliser ces techniques.

8. Flux transfrontières de données

60. Les principes commentés ci-dessus concernent les contextes nationaux spécifiques dans lesquels des données à caractère personnel ou les fichiers contenant des données à caractère personnel sont communiqués par des organismes publics à des tierces personnes. Les sauvegardes et les garanties concernées jusqu'à présent sont fondées

sur des considérations de droit interne. Cependant, l'on ne peut ignorer la communication de données à caractère personnel ou de fichiers contenant des données à caractère personnel détenus par des organismes publics d'un pays à des tierces personnes situées dans d'autres pays. La technologie permet actuellement à des tierces personnes d'accéder, à partir d'un pays A, à des fichiers contenant des données à caractère personnel et détenus par des organismes publics d'un pays B. Les données peuvent par exemple être déchargées d'un pays à un autre. Alternativement, les organismes publics peuvent envoyer des bandes magnétiques par la poste à des tierces personnes résidant dans un autre Etat. En d'autres termes, il est aussi nécessaire de traiter des problèmes de protection des données soulevés, dans ce secteur, dans le cadre de la communication transfrontière de données à caractère personnel ou de fichiers contenant des données à caractère personnel (principe 8.1).

61. Les rédacteurs de la recommandation ont essayé d'adapter les principes de l'article 12 de la Convention sur la protection des données pour fournir des principes spécifiques pour la communication dans ce secteur. Le principe 8 de la recommandation analyse certaines situations dans lesquelles la communication transfrontière peut s'effectuer:

- la communication peut être faite vers le territoire d'un Etat ayant ratifié la convention;
- la communication peut être faite vers le territoire d'un Etat qui, bien que n'étant pas Partie contractante à la convention, jouit néanmoins de dispositions juridiques conformes à la convention et à la présente recommandation;
- la communication peut être faite vers le territoire d'un Etat ne possédant pas de dispositions juridiques conformes à la convention ou à la présente recommandation.

62. Partant de chacune des diverses hypothèses indiquées ci-dessus, les rédacteurs de la recommandation ont fourni le cadre juridique suivant au flux transfrontière de données.

63. Concernant la première hypothèse et conformément aux principes de l'article 12, paragraphe 2, de la Convention N°108, le principe 8.2 de la recommandation établit le principe du libre flux des données. Etant donné qu'une Partie contractante à la convention doit posséder des normes de protection des données compatibles avec les principes de base du traité, il n'y a *a priori* aucune justification pour restreindre le libre flux des données. C'est certainement le cas lorsque l'Etat exportateur est également une Partie contractante. Toutefois, le principe 8 de la recommandation ne se limite pas exclusivement à la situation dans laquelle le pays exportateur est une Partie contractante. Il envisage également les cas où les données à caractère personnel sont communiquées par des Parties non contractantes, y compris les Etats n'ayant pas encore adopté de législation sur la protection des données. Les rédacteurs de la recommandation ont essayé d'encourager tous les pays à accepter le principe du libre flux de données vers les Etats ayant ratifié la Convention N°108.

Les dispositions du principe 8.2 ne portent pas préjudice au droit d'une Partie contractante de déterminer les conditions de transfert de catégories particulières de données à caractère personnel ou de fichiers contenant des données à caractère

personnel conformément aux dispositions de l'article 12, paragraphe 3.a, de la Convention N°108.

64. Le principe 8.3 traite de la situation dans laquelle l'Etat destinataire possède des dispositions juridiques reflétant les principes de base de la Convention N° 108 ainsi que la philosophie de la présente recommandation, mais n'a pas encore ratifié la convention. Certains Etats ont en fait adopté des lois de protection des données conformes à la convention mais n'ont pas encore atteint l'étape consistant à déposer leurs instruments de ratification. Comme le principe 8.2, le principe 8.3 encourage également le libre flux de données vers ces Etats. L'on a estimé que, bien que la ratification de la convention soit d'une absolue nécessité, la situation juridique concernant la protection des données dans ces pays devrait être considérée comme suffisante et la communication transfrontière devrait pouvoir intervenir sans conditions supplémentaires. Pour utiliser la terminologie de la convention, on peut supposer qu'un "niveau de protection équivalent" existe dans ces pays, au moins lorsque les données doivent être exportées d'un territoire des Parties contractantes.

65. Le principe 8.4 traite de la situation dans laquelle le pays de destination n'a pas ratifié la Convention N° 108 et ne possède pas de dispositions juridiques sur la protection des données à caractère personnel, ou du moins pas de dispositions que l'on puisse considérer comme étant compatibles avec les principes de base de la convention. Dans ce cas, et afin de ne pas affaiblir la protection des personnes concernées et ainsi d'amoindrir la portée des principes de protection des données, et notamment les principes énoncés tant dans la convention que dans la présente recommandation, les Etats exportateurs devraient réfléchir à la possibilité d'imposer des restrictions à la communication de données à caractère personnel à des tierces personnes résidant dans ces pays.

66. En premier lieu, les rédacteurs de la recommandation ont suggéré qu'aucune communication n'intervienne en l'absence du consentement écrit, exprès et éclairé de la personne concernée. En outre, ce consentement devrait être révocable en tout temps. L'on a estimé qu'il était justifié d'augmenter le niveau de l'exigence du consentement en incluant le "consentement par écrit" au principe 8.4, étant donné que les données sont communiquées en dehors du territoire de la personne concernée et dans un pays où il est impossible de contrôler l'avenir des données.

67. Le principe 8.4 prévoit également une méthode alternative pour assurer la protection des données dans le cas d'une communication des données vers des pays n'ayant pas encore légiféré en matière de protection des données. La méthode alternative propose que le pays exportateur adopte des mesures qui pourraient garantir l'intégrité des données, y compris le respect des principes énoncés dans la convention et dans la présente recommandation, dans le territoire du pays destinataire. Une des mesures pourrait être d'exiger que la partie importatrice s'engage contractuellement à respecter les principes de protection des données. A ce propos, l'on pourrait faire référence au projet de contrat type élaboré par le Comité consultatif des Parties contractantes à la Convention N° 108. Il convient de souligner que l'utilisation d'un contrat juridique doit être perçue comme une solution d'attente jusqu'à la promulgation de dispositions de protection des données dans le pays de destination et ne doit pas être considérée comme un substitut à la nécessité d'adopter de telles dispositions à un stade quelconque. Afin de permettre de régler des litiges

indépendamment des considérations de droit national, le contrat devrait prévoir un système d'arbitrage indépendant. La compétence des arbitres Indépendants devrait s'étendre jusqu'à permettre à la personne concernée de faire respecter ses droits relatifs à ses données, et de lui octroyer une réparation dans le cas où de tels droits seraient méconnus par la tierce personne. Le principe 8.4 souligne que l'adoption de telles mesures, en tant qu'alternative à l'exigence du consentement écrit, exprès et éclairé de la personne concernée, dépend du fait que la personne concernée ait été informée de la possibilité que ses données pourraient être communiquées à des tierces personnes situées dans des pays non dotés de dispositions de protection des données, lui donnant ainsi la possibilité de s'opposer à la communication.

68. Le principe 8.5 met en lumière un problème particulier soulevé par les possibilités transfrontières d'accès en ligne ou de télédéchargement de données généralement accessibles ou de fichiers contenant des données. Ce problème est encore plus aigu dans le cas d'une communication à des Etats non dotés de législation sur la protection des données. Compte tenu du désir des rédacteurs de la recommandation de préparer un texte technologiquement pertinent, il a été jugé important d'appeler l'attention des législateurs nationaux sur la question de la consultation ou du télédéchargement à partir de l'étranger.

9. Coordination - coopération

69. Dans la partie réservée au préambule, l'on a fait référence à la nécessité de porter la recommandation "à l'attention des autorités établies en vertu d'une législation sur la protection des données ou d'une législation sur l'accès à l'information du secteur public". Le principe 9 de la recommandation encourage la coordination accrue du rôle de ces autorités en vue d'assurer une approche cohérente de la communication à des tierces personnes de données à caractère personnel ou de fichiers contenant des données à caractère personnel détenus par des organismes publics. Le dialogue encouragé par le principe 9 devrait permettre aux organismes concernés de s'informer sur les conditions qui régissent la communication. A titre d'exemple: la communication de données à caractère personnel selon les dispositions régissant la liberté d'information est invariablement restreinte lorsque la communication est susceptible de causer un préjudice à la vie privée de la personne concernée. L'interprétation d'une telle disposition n'est habituellement pas définie dans la législation sur la liberté d'information. L'on estime que les autorités chargées de l'interprétation de la disposition pourraient utilement se fonder sur les conditions énoncées par les autorités chargées de la protection de données sur l'utilisation qui peut être faite des données à caractère personnel qu'elles ont déclarées, notifiées ou enregistrées. Etant donné que les autorités responsables de la protection des données peuvent limiter l'utilisation qui peut être faite par les organismes publics, y compris la communication, des fichiers contenant des données à caractère personnel qu'ils détiennent, l'on a estime qu'il serait approprié que l'organisme agissant selon la législation sur la liberté d'information prenne note de ces conditions.