COMMISSION CONSULTATIVE DE LA PROTECTION DE LA VIE PRIVEE

N. Réf. 10527/L/S/49

AVIS N° 90/093 DU 16 NOVEMBRE 1990

Objet : Proposition de directive du Conseil des Communautés européennes relative à la protection des personnes à l'égard du traitement des données à caractère personnel[1].

La Commission consultative de la protection de la vie privée,

Vu l'arrêté royal n° 141 du 30 décembre 1982 créant une banque de données relatives aux membres du personnel du secteur public, notamment l'article 6, et la loi du 8 août 1983 organisant un Registre national des personnes physiques, notamment l'article 12,

A émis le 9 novembre 1990 l'avis suivant :

I. Contexte dans lequel s'inscrit la proposition de directive

1°)La protection des données à caractère personnel peut encore être considérée aujourd'hui comme une branche récente du droit.

Ce n'est, en effet, que dans les années soixante-dix qu'elle est apparue sous sa forme présente.

Le caractère récent de la protection des données à caractère personnel peut évidemment être expliqué par le développement très rapide de l'informatique, puis de la télématique, au cours des deux dernières décennies et des possibilités nettement accrues de collecte, de traitement et de rapprochement de données de natures diverses qui en ont résulté.

[1] Proposition COM (90) 314 final - SYN 287 du 13 septembre 1990.

Par le passé, seules quelques catégories particulières d'informations dont la divulgation était, en elle-même, susceptible de porter atteinte à certains intérêts de la personne physique à laquelle elles se rapportaient faisaient l'objet de mesures de protection sanctionnées juridiquement[2].

L'adoption rapide de dispositions relatives à la protection des données à caractère personnel a démontré que le droit peut, lorsque cela apparaît impératif, être complété de manière à maintenir le respect de libertés fondamentales peu après l'apparition d'une menace à leur égard.

Ainsi fut établie, dès le 28 janvier 1981, la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Cette très importante convention, instrument majeur de la coopération internationale dans un domaine fondamental[3], a été, jusqu'à présent, ratifiée par 10 Etats, dont 7 sont membres de la Communauté européenne.

Il faut, pour être complet, ajouter que les Pays-Bas, qui n'ont pas encore ratifié cette convention, disposent d'une législation générale sur la protection des données à caractère personnel entrée en vigueur depuis le 1er juillet 1990.

Au contraire, l'Espagne a ratifié la convention depuis le 31 janvier 1984, mais elle n'a pas encore rendu ses principes applicables dans son droit interne[4].

Enfin, le Portugal a inscrit le principe de la protection des données dans sa Constitution, mais il n'a pas ratifié la Convention n° 108 et il ne dispose d'aucune loi en la matière.

2°)Le grand marché intérieur entrera en vigueur, entre les Etats membres de la Communauté européenne, le 1er janvier 1993[5].

L'achèvement du marché intérieur repose sur quatre libertés fondamentales : la libre circulation des biens, des services, des personnes et des capitaux.

Ce quadruple principe de libre circulation complété par des dispositions portant sur la liberté d'établissement des personnes physiques et morales[6] - ne peut être réalisé

---

[2]Art. 458 du Code pénal, dès 1865. A l'échelle du Conseil de l'Europe, l'article 8 de la Convention européenne des droits de l'homme.

[3]Il existe d'autres instruments juridiques internationaux en matière de protection des données à caractère personnel; toutefois, aucun d'entre eux ne lie les Etats auxquels ils s'adressent.

[4]La Convention n° 108 n'est pas entièrement self-executing : diverses dispositions internes sont indispensables à sa mise en oeuvre intégrale.

[5]Article 8A du Traité de Rome inséré par l'article 13 de l'Acte unique.

[6]Titre III du Traité de Rome et l'important droit dérivé qui s'y rapporte, dont la directive du 21 décembre 1988 relative à un système général de reconnaissance des diplômes d'enseignement supérieur qui sanctionnent des formations d'une durée minimale de trois ans.

efficacement que s'il a comme corollaire la libre circulation des données, parmi lesquelles les données à caractère personnel, au sein de la Communauté européenne[7].

Or, la Convention n° 108, ratifiée, rappelons-le, par 7 Etats de la Communauté européenne, prévoit, à l'article 12, 3, qu'une Partie à cette Convention peut interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel :

"a. dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection suffisante;

b. lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non-contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe."

Rien n'est prévu concernant les autres flux transfrontières vers des Etats non-contractants; ceux-ci peuvent donc être soumis à autorisation ou interdits.

La libre circulation de données à caractère personnel ne peut, par conséquent, être assurée à l'intérieur de la Communauté européenne que si une protection équivalente à celle dont elles bénéficient dans l'Etat d'origine - où se trouve l'expéditeur - leur est accordée dans l'Etat destinataire[8] et si celui-ci a ratifié la Convention.

Aussi le seul moyen de réaliser la libre circulation des données à caractère personnel au sein de la Communauté européenne consiste-t-il à s'assurer que ce niveau de protection équivalente est atteint dans chacun des Etats membres. D'où la proposition de directive qui est analysée dans cet avis, qui vise au rapprochement des législations des Etats membres dans le domaine de la protection des données à caractère personnel[9].

Si tous les Etats de la Communauté européenne ne disposaient pas, le premier janvier 1993, d'une législation efficace en ce domaine, la libre circulation des données à caractère personnel continuerait à être entravée dans la Communauté et la réalisation du marché intérieur serait, au moins en partie, compromise.

La proposition de directive précitée se révèle donc extrêmement importante pour l'avenir de l'Europe.

3°)La proposition de directive a été adoptée par la Commission le 13 septembre 1990 (document Com (90) 314 final).

---

[7]Voy. notamment, à ce sujet, les dispositions qui ont dû être introduites dans les accords de Schengen (instituant un laboratoire concernant un nombre limité d'Etats de la Communauté européenne), en particulier le S.I.S.

[8]Le même principe est évidemment applicable aussi lorsque ces données sont transmises d'un Etat ayant ratifié la convention n° 108 vers un Etat non-membre de la Communauté européenne.

[9]Voy. d'ailleurs son exposé des motifs, pp. 16 et 17 du doc. COM (90) 314 final.

Ses grands principes ont été présentés publiquement le 19 septembre 1990 à l'occasion de la XIIe Conférence Internationale des Commissaires à la Protection des Données qui s'est tenue, à l'invitation de la Commission Nationale (française) de l'Informatique et des Libertés, au Palais du Luxembourg à Paris.

II - Examen des articles

CHAPITRE I - DISPOSITIONS GENERALES

Article 1 (objet)

L'article 1, paragraphe 1, de la proposition de directive impose aux Etats membres de la C.E.E. d'assurer la protection de la vie privée des personnes à l'égard du traitement de données à caractère personnel contenues dans des fichiers conformément aux dispositions de cette proposition de directive.

Les Etats qui ne disposent pas encore d'une législation en la matière ou qui ne disposent, pour l'instant, que d'une législation partielle devront donc en adopter une et celle-ci devra être conforme aux dispositions de la directive.

Quant aux Etats qui disposent déjà d'une législation de protection des données à caractère personnel, ils devront, le cas échéant, la modifier en fonction de la directive.

Cette obligation reflète la volonté légitime d'harmoniser le droit des Etat membres dans ce domaine.

Il est nécessaire que cette harmonisation s'opère de manière à garantir un haut niveau de protection des données à caractère personnel.

C'est d'ailleurs ce que déclare la Commission des Communautés européennes[10] dans sa communication relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans la Communauté et à la sécurité des systèmes d'information[11].

Les dispositions contenues dans la proposition de directive doivent donc constituer des moyens efficaces d'assurer ce haut niveau de protection. Elles doivent, à cet effet, reprendre et améliorer les principes établis dans les Etats membres dont le droit positif assure les niveaux de protection des données les plus élevés.

Ceci s'avère d'autant plus indispensable que l'article 1, paragraphe 2, dispose que les Etats membres ne peuvent restreindre ou interdire la libre circulation des données entre eux.

Cette obligation imposée aux Etats membres s'inscrit naturellement dans le cadre du

[10] Dénommée ci-après la Commission européenne.

[11] pp. 2 et 3 du doc. Com (90) 314 final.

besoin de garantir la libre circulation des données à l'intérieur du marché unique.

Elle a comme corollaire la nécessité que chacun des Etats membres assure un niveau de protection élevé équivalent et, par conséquent, que la directive en projet leur impose de mettre en place ou de renforcer leur niveau de protection.

Les dispositions de la directive jouent, par conséquent, un rôle fondamental puisque ce sont elles qui vont guider les Etats dans cette réalisation.

Article 2 (définitions)

Cet article fournit les définitions de huit termes et expressions employés dans la directive. Une attention particulière doit, dès lors, y être accordée.

a) Données à caractère personnel

La définition de la notion de "données à caractère personnel" reprend celle présentée par la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel :

"Toute information concernant une personne physique identifiée ou identifiable".

La Commission se réjouit de ce que la proposition de directive conserve la définition large fournie par la Convention, ce qui assure l'unité d'interprétation de la notion fondamentale de "données à caractère personnel".

Par ailleurs, la définition mentionnée dans la proposition de directive précise qu'"est notamment réputée identifiable une personne qui peut être identifiée par référence à un numéro d'identification ou une information similaire".

La Commission considère que cette présomption complémentaire est très utile en raison du recours croissant à des numéros personnels d'identification, en particulier en Belgique où pareil numéro a été mis en place au niveau national par la loi du 8 août 1983 organisant un registre national des personnes physiques.

La Commission estime que doit ainsi être considérée comme une donnée à caractère personnel toute information associée à un procédé d'identification directe ou indirecte de la personne à laquelle elle se rapporte.

L'information qui porte sur une caractéristique propre à une seule personne doit être considérée à la fois comme une information à caractère personnel et comme un procédé d'identification indirecte impliquant que les autres informations qui y sont éventuellement associées sont, elles aussi, des données à caractère personnel.

b) Rendre anonyme

Le but de la définition de l'expression "rendre anonyme" est de déterminer quand une donnée initialement à caractère personnel doit cesser d'être considérée comme telle.

Aux termes de la définition, une information devient anonyme lorsqu'elle ne peut plus être associée à une personne physique déterminée ou déterminable, ou moyennant seulement un effort excessif en personnel, en frais et en temps.

Cette définition correspond approximativement à la conception généralement admise par les experts en matière de protection de données.

La Commission préférerait toutefois que le mot "excessif" soit remplacé par celui de "déraisonnable".

En effet, l'emploi du terme "excessif" implique une référence au niveau qui sépare l'effort excessif de celui qui ne l'est pas. Il s'agit là d'une notion extrêmement subjective qui pourrait mener à une exclusion trop rapide de certaines informations de la catégorie fondamentale des "données à caractère personnel".

Bien qu'également subjectif, le terme "déraisonnable" renforce l'intensité de l'effort à fournir pour que la personne à laquelle se rapporte l'information soit déterminable.

Il faut, en effet, tenir compte de la variabilité de l'effort qui peut être supporté en fonction des différences entre les personnes ou organismes qui l'accomplissent : l'effort qui peut paraître excessif pour certaine administration publique peut être considéré comme normal ou rentable par une entreprise de marketing, voire par un détective privé.

Le terme déraisonnable soulignerait, au contraire, que l'information ne peut être considérée comme anonyme que si l'effort à fournir pour la rattacher à une personne déterminable n'est raisonnable pour personne.

Ainsi, une donnée qui n'aurait pas de caractère personnel en raison de l'effort à fournir par un organisme pour la rapprocher d'une personne déterminée ne pourrait être communiquée à un tiers pour qui le même effort serait rentable.

c) Fichier

La définition du "fichier" correspond à celle qui est généralement admise.

La Commission apprécie particulièrement la précision qu'un fichier peut être constitué par des données à caractère personnel réparties sur plusieurs sites, ce qui répond à la décentralisation informatique.

La Commission constate, en outre, avec satisfaction que la définition du fichier englobe, comme l'avant-projet de loi belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fichiers tenus manuellement.

En effet, les progrès réalisés dans la technique du scanning rendent la distinction entre les fichiers manuels et les fichiers automatisés de plus en plus théoriques puisque les données contenues dans un fichier manuel peuvent ainsi aisément faire l'objet de traitements automatisés.

d) Traitement

La Commission se rallie à la définition du "traitement" des données, qui vise

notamment les opérations effectuées sans l'aide de procédés automatisés.

Elle relève que sont, entre autres, considérés comme traitements de données leur interconnexion, leur communication, leur verrouillage et leur effacement, ce qui apporte une précision très importante.

e et f) Les définitions figurant aux litteras e et f n'appellent pas de commentaire particulier.

g et h) Secteur public et secteur privé

Les définitions du secteur public et du secteur privé se révèlent d'autant plus importantes que la proposition de directive opère une distinction, quant au champ d'application de certaines de ses dispositions, entre ces deux secteurs.

La Commission apprécie très favorablement que sont exclues de la définition du secteur public les entités de droit public qui participent à une activité industrielle ou commerciale.

Elle relève, par ailleurs, que les organismes et entités de droit privé qui participent à l'exercice de l'autorité publique sont soumis aux dispositions de la directive visant le secteur public.

Elle regrette évidemment qu'il ressort de la combinaison des deux définitions que les personnes physiques, les personnes morales de droit privé et les associations sont exclues du champ d'application de la directive proposée lorsqu'elles n'exercent pas d'activité industrielle ou commerciale, mais elle comprend que cette exclusion résulte des compétences limitées qui sont attribuées aux institutions européennes en vertu du Traité de Rome.

Gestionnaire du fichier

La Commission regrette qu'à côté du "responsable du fichier", la proposition de directive ne comprenne pas également une définition du "gestionnaire du fichier", c'est-à-dire de la personne sous l'autorité de laquelle sont accomplis les divers traitements portant sur les données du fichier.

La notion de "gestionnaire du fichier" aurait ainsi pu être introduite dans différentes dispositions de la directive proposée dans lesquelles la seule référence au "responsable du fichier" est susceptible de se révéler trop étroite.

Article 3 (champ d'application)

Le champ d'application de la directive proposée est déterminé par référence aux fichiers.

Il s'agit d'une innovation majeure par rapport à la Convention du Conseil de l'Europe et par rapport à de nombreuses législations internes, qui se réfèrent, elles, à la notion de "traitement".

La définition du champ d'application par référence aux fichiers est susceptible de faciliter la mise en oeuvre pratique de certaines dispositions; il est infiniment plus facile d'imposer et de contrôler la déclaration d'un fichier que celle d'un traitement de données.

Néanmoins, il faut remarquer que le risque pour la vie privée des individus réside, au-delà du fichier lui-même, dans les traitements qui sont appliqués aux données.

Il faut aussi remarquer qu'un même fichier peut, dans certaines circonstances, faire l'objet de traitements très diversifiés, dont certains peuvent présenter plus de risques pour la vie privée que d'autres.

La Commission ne nie pas qu'il soit nécessaire que plusieurs dispositions de la proposition de directive se réfèrent expressément à la notion de fichier, mais elle considère que définir également le champ d'application par rapport à ce critère pourrait limiter trop strictement l'étendue de ce champ d'application.

Des brèches pourraient ainsi se révéler dans le système protecteur que la proposition de directive tend à mettre en place.

Elle recommande, par conséquent, que le champ d'application soit redéfini en faisant référence au concept de traitement des données à caractère personnel.

Elle suggère que le texte ci-dessous remplace le texte actuel de l'article 3, 1 :

"Les Etats membres appliquent les dispositions de la présente directive à tout traitement de données à caractère personnel du secteur privé et du secteur public, à l'exclusion des traitements du secteur public qui ne relèvent pas du champ d'application du droit communautaire".

Par ailleurs, elle estime que les exclusions figurant à l'article 3, 2, sont justifiées. La phrase introductive de ce paragraphe devrait toutefois viser les "traitements accomplis sur des fichiers" au lieu de ne mentionner que les fichiers.

Article 4 (droit applicable)

La Commission regrette la référence exclusive au fichier - et au responsable du fichier - qui apparaît également dans cette disposition.

Outre cette réserve, la Commission regrette vivement que les paragraphes 1, b, et 2, excluent l'application des dispositions de la directive proposée lors de l'utilisation et de la consultation sporadiques de "fichiers" localisés dans des pays tiers.

Le terme "sporadique" est susceptible de faire l'objet d'interprétations divergentes.

Il réduit, à nouveau, le champ d'application de la directive et il fait apparaître une certaine insécurité juridique tant dans le chef des "responsables des fichiers" et autres

"utilisateurs" de fichiers que dans celui des sujets des données, ces derniers pouvant d'ailleurs être aussi des ressortissants d'Etats membres de la Communauté européenne même lorsque les "fichiers" sont localisés dans des pays tiers.

La Commission regrette aussi l'emploi de l'expression de "niveau de protection **adéquat**"[12].

La Commission propose que l'article 4, 1, soit rédigé de la manière suivante :

"Chaque Etat membre applique les dispositions de la présente directive :

(a) -à tout traitement de données à caractère personnel accompli sur son territoire;
(b) -à toute personne résidant sur son territoire qui procède depuis ce territoire à un traitement de données à caractère personnel à l'aide d'un fichier localisé dans un pays tiers dont la législation ne présente pas un niveau de protection équivalente à celle de l'Etat à partir duquel le traitement est accompli.

Quant au paragraphe 3, il mérite un examen particulier.

Il est fondé sur le principe de l'équivalence des mesures de protection en vigueur dans les différents Etats membres de la Communauté européenne, équivalence que vise d'ailleurs à établir la directive proposée, et il ne constitue qu'un cas d'application particulier du principe énoncé à l'article 1, paragraphe 2.

La Commission est extrêmement favorable à ce principe.

Elle considère néanmoins qu'il n'est souhaitable de l'appliquer que si le niveau de protection globalement instauré par la directive est suffisamment élevé. Or, elle exprime de sérieux doutes à ce sujet en l'état actuel du texte proposé[13].

Elle estime donc que l'article 4, 3, doit être maintenu, mais elle réclame, comme corollaire, que plusieurs autres des dispositions proposées soient revues de manière à améliorer le système de protection des données.

CHAPITRE II - LEGITIMITE DU TRAITEMENT DANS LE SECTEUR PUBLIC

Article 5 (principes)

L'article 5 est destiné à mettre en oeuvre le principe fondamental qui est prévu par la Convention du Conseil de l'Europe[14] selon lequel le traitement des données à caractère personnel doit être légitime.

A cet effet, il énonce plusieurs critères permettant d'apprécier si un traitement de données effectué dans le secteur public doit être considéré comme légitime.

L'article 5, 1, a,[15] dispose que "l'établissement d'un fichier et tout autre traitement de

[12] Voy. infra, le commentaire de l'article 24.

[13] Voy. infra.

[14] Art. 5, a, de la Convention.

[15] La Commission s'interroge sur la raison de la numérotation d'un paragraphe qui est le seul repris dans l'article 5.

données à caractère personnel sont légitimes dans la mesure où ils sont nécessaires pour l'exécution des missions de l'autorité publique responsable de ce fichier".

Le traitement de données n'est donc légitime que s'il est nécessaire pour l'exécution d'une ou plusieurs des missions qui sont confiées à l'autorité publique qui est responsable du fichier.

La Commission approuve ce principe, mais elle estime qu'il est mal formulé en raison de la référence, une fois de plus, au "fichier". Qu'en est-il si une autorité publique autre que le responsable du fichier a besoin de procéder à un traitement portant sur certaines des données stockées dans le fichier ? Le critère fourni par la proposition de directive pour apprécier la légitimité d'un traitement de données doit, dans cette optique, être considéré comme trop étroit[16].

La Commission tient cependant surtout à mettre l'accent sur le fait que, bien qu'elle approuve le principe précité, elle le considère comme insuffisant.

Il lui paraît, en effet, insuffisant qu'un traitement de données soit - simplement - nécessaire pour l'exécution des missions du responsable du fichier pour qu'il doive automatiquement être considéré comme légitime.

Il faut encore que, parmi les traitements envisageables pour exécuter l'une de ces missions, il apparaisse comme celui qui porte le moins atteinte au droit de l'individu à la protection des données qui le concernent.

Il faut aussi que ce traitement soit exécuté en prenant toutes les mesures propres à réduire au maximum les atteintes à ce droit.

Il est indispensable qu'un équilibre soit établi entre l'efficacité avec laquelle la mission d'une autorité publique peut être accomplie et la nécessité de protéger les données à caractère personnel.

Enfin, la Commission présume que, par "missions de l'autorité publique", la proposition de directive ne vise que les missions qui sont confiées à cette autorité par ou en vertu d'une disposition légale ou réglementaire. Il serait opportun de le préciser dans le principe en cause.

A côté du principe de base énoncé à l'article 5, 1, a, la proposition de directive prévoit quatre possibilités de "rattrapage" pour reconnaître la légitimité des traitements de données qui ne répondent pas au critère du second principe.

La première de ces possibilités est constituée par le consentement de la personne concernée. Il s'agit du "consentement informé" qui est décrit à l'article 12.

La Commission peut être d'accord avec cette possibilité de considérer un traitement comme légitime. Elle souhaite toutefois qu'il s'agisse, en toutes circonstances, d'un consentement donné librement par le sujet des données, sans que l'autorité publique n'abuse de sa qualité en exerçant l'une ou l'autre forme de pression sur l'intéressé.

---

[16]Voy. toutefois, le commentaire de l'art. 5, 1, b, 2è tiret.

La seconde possibilité prévue à l'article 5, 1, b, vise l'hypothèse évoquée précédemment dans laquelle une autorité - ou un organisme privé - autre que le responsable du fichier doit procéder à un traitement pour remplir l'une de ses missions légales.

La Commission se demande pourquoi les précisions qui figurent dans cette disposition ("sur la base du droit communautaire, ou d'une loi ou d'un acte pris en application d'une loi conforme à la présente directive", "(loi,...) qui l'autorise et en fixe les limites") n'ont pas été également introduites dans le principe de l'article 5, 1, a.

Elle estime que les conditions dans lesquelles un traitement peut être considéré comme légitime doivent être identiques pour le responsable du fichier et pour les autres autorités publiques.

Elle préconise donc la fusion des principes de l'article 5, 1, a, et 5, 1, b, 2ème tiret, dans une seule disposition qui tienne compte des remarques qu'elle a émises au sujet du principe contenu à l'article 5, 1, a.

L'article 5, 1, b, 3ème tiret, qui affirme la légitimité d'un traitement de données lorsqu'"un intérêt légitime de la personne concernée ne s'oppose pas à ce changement de finalité, revient à vider de son sens le principe du respect des finalités.

La Commission demande la suppression de cette disposition.

Enfin, la Commission exprime son accord avec le dernier principe de l'article 5, mais elle souhaiterait que seules des autorités publiques soient admises à l'invoquer et que celles parmi ces autorités qui y soient admises soient définies avec précision (par exemple : "les autorités publiques investies d'une compétence en matière de police").

La Commission souhaiterait, en outre, qu'il soit mentionné que seules les données **pertinentes** pour prévenir la menace imminente pour l'ordre public ou l'atteinte sérieuse au droit d'autrui peuvent être traitées sur base de ce principe.

Elle recommande, par ailleurs, que les types d'atteinte sérieuse et la nature du droit d'autrui soient déterminés avec plus de précision.

Article 6 (communication de données détenues par le secteur public.)

L'article 6 détermine les cas dans lesquels le responsable d'un fichier du secteur public est autorisé à communiquer certaines des données du fichier soit à d'autres entités du secteur public, soit à une personne du secteur privé.

Puisque l'article 5 établit les principes auxquels un traitement est soumis pour être reconnu légitime et que l'article 6 porte sur la légitimité du traitement ayant pour objet la communication de données, il faut considérer que l'article 6 déroge à l'article 5 dans le cas spécifique de la communication de données et que, par conséquent, celle-ci ne peut intervenir que lorsque les conditions énoncées à l'article 6 sont **également** remplies.

a) Communication à une entité du secteur public

L'article 6, 1, (a), dispose que la communication de données à une autre entité du

secteur public n'est légitime que si elle est nécessaire pour l'exercice des missions soit de l'entité qui communique les données, soit de celle qui demande leur communication.

Comme elle l'a déjà exprimé à propos de l'article 5, 1, (a), la Commission considère qu'il n'est pas suffisant qu'un traitement de données, y compris celui ayant pour objet la communication de données, soit nécessaire pour l'exécution des missions d'une entité du secteur public pour qu'il doive automatiquement être considéré comme légitime.

La Commission réitère, par conséquent, au sujet de cette disposition les remarques faites au sujet de l'article 5, 1, a et b, 2ème tiret : il faut que, parmi les traitements envisageables pour exécuter une mission du secteur public, le traitement choisi apparaisse comme celui qui porte le moins atteinte au droit de l'individu à la protection des données qui le concernent; il faut que ce traitement soit exécuté en prenant toutes les mesures propres à réduire au maximum les atteintes à ce droit; enfin, il est indispensable qu'un équilibre soit établi entre l'efficacité avec laquelle la mission d'une autorité publique peut être accomplie et la nécessité de protéger les données à caractère personnel.

La Commission est consciente que l'article 6, 2, complète le paragraphe 1, a, en permettant aux Etats membres de préciser les conditions dans lesquelles la communication de données est légitime.

Elle estime cependant sur la portée qui doit être attribuée à ce second paragraphe.

La proposition de directive étant destinée à mettre en place un régime protecteur des données à caractère personnel dans l'ensemble de ces Communautés européennes et la Commission européenne insistant, dans l'exposé des motifs, sur le haut niveau de protection qui devrait être atteint, la Commission ose espérer que l'article 6, 1, (a), doit être considéré comme un seuil minimal de protection des données en-dessous duquel les précisions des Etats membres ne pourraient descendre et que les précisions apportées sur base du paragraphe 2 ne peuvent que donner une portée plus restrictive à la notion de communication légitime.

Que cette interprétation soit, ou non, la bonne, l'article 6, 2, sera la source de disparités entre les législations des Etats membres en ce qui concerne les conditions dans lesquelles la communication de données au sein du secteur public doit être considérée comme légitime.

Or, la Commission suppose que, dans un instrument législatif émanant des Communautés européennes, l'extrait de phrase affirmant que "la communication de données à caractère personnel contenues dans des fichiers d'une entité du secteur public n'est légitime que si cela est nécessaire pour l'exercice des missions de l'entité du secteur public qui communique ou qui demande la communication "peut notamment viser la communication de données entre entités du secteur public d'Etats membres différents.

L'article 6, 1, (a), et 2, vise donc, entre autres, la communication de données d'une entité relevant du secteur public d'un Etat membre à une entité relevant du secteur public d'un autre Etat membre, un type de communication dont la fréquence est en pleine croissance, en particulier dans certains domaines tels que celui de la sécurité sociale, et ne peut qu'augmenter après la mise en place du marché intérieur.

Dans le cas assez probable où les conditions fixées en vertu de l'article 6, 2, par les Etats dont relèvent respectivement les entités du secteur public concernées par une

communication seraient différentes, comment parviendrait-on à déterminer si la communication en cause peut ou doit être considérée comme légitime?

La Commission estime, par conséquent, qu'il serait souhaitable que la directive elle-même détermine les conditions - strictes - dans lesquelles une communication est légitime.

Le paragraphe premier devrait être revu en conséquence, en tenant compte des remarques que la Commission a formulées ci-avant et le paragraphe 2 devrait être supprimé.

A défaut, le paragraphe 2 devrait être complété par une règle portant sur les conflits de lois qui impose de ne retenir que les conditions les plus strictes. Sinon, ce serait l'article 1er, 2, qui deviendrait applicable, ce qui aboutirait à ne retenir, dans chaque cas d'espèce, que les conditions les plus souples pour admettre la légitimité de la communication.

En tout état de cause, l'article 6, 1, (a), devrait être beaucoup plus strict et précis.

b) Communication à une personne du secteur privé

L'article 6, 1, (b) dispose que la communication de données à caractère personnel contenues dans des fichiers d'une entité du secteur public faite sur demande d'une personne physique ou morale du secteur privé est légitime si cette personne invoque un intérêt légitime et à condition que l'intérêt de la personne concernée ne prévale pas.

La Commission apprécie favorablement que, dans cette hypothèse-ci, il soit précisé "à condition que l'intérêt de la personne concernée ne prévale pas".

Cependant, la manière dont la disposition est rédigée est génératrice de subjectivité et, ainsi, elle entraîne l'insécurité juridique et, surtout, elle n'atteint pas l'objectif de protection des données que leur sujet est légitimement en droit d'attendre.

En effet, elle met en balance l'intérêt légitime de la personne privée qui demande la communication et l'intérêt du sujet des données. Ces deux notions sont très subjectives et la disposition est, dès lors, susceptible d'interprétations divergentes, dans des sens plus ou moins protecteurs des données.

Or, il faut avoir égard à deux éléments importants : la nature des données et le principe du respect des finalités.

En ce qui concerne la nature des données, les différents fichiers du secteur public peuvent contenir, en raison des facilités dont dispose précisément le secteur public pour collecter les données de toutes natures auprès de diverses sources, des données qui, sans rentrer dans les catégories particulières de données sensibles visées à l'article 17, 1, et 3, présentent, en raison soit de leur nombre élevé, soit de leur nature, un caractère aigu.

Par ailleurs, les raisons pour lesquelles des données sont introduites dans un fichier du secteur public et les traitements auxquels elles y sont soumises différent, en général, fortement des motivations et des traitements du secteur privé.

La communication de données du secteur public au secteur privé implique, par conséquent, fréquemment un changement de finalité.

Or, la Convention du Conseil de l'Europe dispose que les données sont enregistrées pour des **finalités déterminées** et légitimes et **ne sont pas utilisées de manière incompatible avec ces finalités**[17].

C'est le principe même du respect des finalités qui, dans de nombreux cas, pourrait être remis en question par l'article 6, 1, (b), de la proposition de directive.

En effet, si l'expression "pas utilisées de manière incompatible avec ces finalités" employée dans la Convention permet de procéder à un traitement destiné à atteindre une finalité connexe à la finalité déterminée initialement, elle interdit un changement de finalité aussi important que celui qui résulterait le plus souvent de la communication de données du secteur public à des personnes du secteur privé.

Si, par exemple, des données à caractère financier sont collectées afin de calculer le montant de cotisations sociales ou d'établir le droit à la pension de retraite d'un individu, la communication de ces données à des entreprises de marketing direct ou de mailing désireuses de déterminer si les ressources pécuniaires d'un client potentiel lui permettent d'acquérir un bien ou un service qu'elles envisagent de lui proposer, il y a manifestement un détournement de finalité.

Pourtant, dans ce cas, une interprétation laxiste de l'article 6, 1, (b), pourrait amener à considérer que ces entreprises ont un intérêt légitime - la poursuite de leur but social - à recevoir communication des données sur lequel l'intérêt de la personne concernée ne prévaudrait pas.

La Commission estime, par conséquent, que la communication de données du secteur public au secteur privé devrait être soumise à des conditions beaucoup plus restrictives.

La Commission émet, par ailleurs, les mêmes remarques au sujet du second paragraphe en tant qu'il vise la communication de données aux personnes du secteur privé que celles qu'elles a faites à son sujet en ce qui concerne la communication à des entités du secteur public.

Enfin, la Commission approuve le paragraphe 3, sous la réserve que l'autorisation de l'autorité de contrôle ne devrait pas remplacer, mais coexister, avec l'information des sujets des données.

L'accord de la Commission avec cette disposition n'atténue pas ses critiques à l'égard des deux paragraphes précédents.

Article 7 (notification à l'autorité de contrôle)

La Commission approuve le principe établi par l'article 7, à savoir la tenue, par l'autorité de contrôle, d'un registre des fichiers du secteur public qui peut être consulté par toute personne.

Toutefois, l'article 7 ne porte que sur les fichiers dont les données à caractère

[17] Art. 5, b.

personnel sont susceptibles d'être communiquées et il permet aux Etats membres d'étendre à d'autres fichiers l'obligation de notification à l'autorité de contrôle. La Commission préférerait que cette obligation soit imposée par la directive elle-même à propos de tous les fichiers publics - au sens de la directive - faisant l'objet d'un traitement automatisé et, comme le prévoit l'article 7, aux fichiers manuels dont les données sont susceptibles d'être communiquées.

La Commission peut accepter les exceptions prévues à l'article 7, 3 par référence à l'article 15, paragraphe premier, sauf en ce qui concerne les raisons mentionnées à l'article 15, 1, e, qui ne lui paraissent pas de nature à justifier la limite à la consultation du registre; la Commission craint d'ailleurs que ces raisons soient interprétées de manière extensive.

CHAPITRE III - LEGITIMITE DANS LE SECTEUR PRIVE

Article 8 (principes)

L'article 8, 1, qui suppose l'existence d'un principe général - le consentement du sujet des données - et établit trois hypothèses dans lesquelles un traitement de données à caractère personnel dans le secteur privé doit être considéré comme légitime par dérogation au principe général qu'il vient d'établir.

En ce qui concerne les trois hypothèses qui dérogent à ce principe, porte sur le traitement qui s'inscrit dans le cadre d'un contrat ou d'une relation de confiance quasi-contractuelle avec la personne concernée et qui est nécessaire à l'exécution de ce contrat ou de cette relation.

Bien que la Commission soit consciente de la nécessité d'accomplir certains traitements de données lors de l'exécution de certains contrats, elle estime que le consentement informé - au sens de la proposition de directive - de la personne concernée doit avoir été recueilli préalablement, en ayant, au besoin, informé la personne concernée que le contrat ne pouvait être conclu sans ce consentement.

Il est, en effet, indispensable que la personne concernée ne s'engage pas dans des relations contractuelles sans être informée des traitements de données la concernant qui peuvent être nécessaires à l'exécution de ces relations contractuelles.

L'existence de certains traitements de données peut constituer, pour cette personne, un facteur d'appréciation de l'intérêt qu'elle a à conclure, ou non, un contrat dont l'exécution rend ces traitements nécessaires.

La Commission estime, dès lors, qu'il n'y a pas lieu de déroger au principe de base du consentement du sujet des données dans l'hypothèse visée à l'article 8, 1, a.

Elle estime, de même, que ce consentement est nécessaire lorsque des données à caractère personnel doivent être collectées préalablement à la conclusion d'un contrat (contrats de prêt, d'ouverture de crédit ou d'assurance, notamment).

En ordre subsidiaire, elle tient à relever l'ambiguïté des termes "relation de confiance quasi-contractuelle", qui pourraient donner lieu à une interprétation trop large.

La seconde hypothèse réglée à l'article 8, 1, ne présente aucun problème.

Par contre, bien que la Commission apprécie favorablement la place réservée à l'intérêt de la personne concernée dans la troisième hypothèse, elle souhaite que cette dernière soit restreinte aux traitements conformes au principe du respect des finalités.

L'article 8, 2, porte sur le cas des traitements qui ont pour objet la consultation ou la communication de données.

La Commission considère que ce type de traitement doit, en premier lieu, être reconnu comme légitime en vertu du paragraphe premier.

Le responsable du fichier doit, en outre, s'assurer, en vertu du second paragraphe, que ce type de traitement n'est pas incompatible avec la finalité du fichier et qu'il ne porte pas atteinte à l'ordre public.

La Commission approuve cette obligation mais elle souhaite qu'elle soit formulée de façon positive en ce qu'elle porte sur la compatibilité du traitement avec la finalité du fichier :

" ... il incombe au responsable du fichier de s'assurer que toute communication **est compatible** avec la finalité du fichier et qu'elle ne porte pas atteinte à l'ordre public".

Quant à l'article 8, 3, il suscite les mêmes remarques que l'article 6, 2.

Article 9 (information de la personne concernée)

L'article 9, 1, impose aux Etats membres de prévoir que, lors de la première communication ou lors de l'ouverture d'une consultation en ligne, le responsable en informe la personne concernée et indique également la finalité du fichier, les types de données qui y figurent et son nom et son adresse.

La Commission ne peut qu'approuver le principe de l'information de la personne concernée.

Elle regrette toutefois vivement le moment auquel la proposition de directive impose cette information : celui de la première communication ou de l'ouverture d'une consultation en ligne.

Elle estime que c'est dès le moment où les données sont collectées en vue de leur incorporation dans le fichier ou d'un quelconque traitement que doit intervenir l'information du sujet des données.

Celui-ci doit, en effet, avoir le droit de savoir que des données le concernant sont enregistrées ou font l'objet d'un autre traitement sans attendre que ces données soient, en outre, éventuellement mises à la disposition d'autres tiers.

Il se révèle d'ailleurs étrange qu'aux termes de l'article 9, 1, de la proposition de directive, le "responsable" - du fichier, présume la Commission - n'informe le sujet des

données de la **finalité** du fichier et des types de données qui y figurent - et, en fait, de l'existence du fichier - que le jour où il met les données à la disposition de tiers.

Il est encore plus étrange d'accorder, au paragraphe 3, au sujet des données la possibilité d'objecter contre tout traitement de données alors qu'il ignore que des données le concernant font l'objet de traitements aussi longtemps qu'elles ne sont pas communiquées à des tiers ou mises à leur disposition par l'ouverture d'une consultation en ligne.

L'obligation d'information lors de la collecte, ne permet, en effet, pas au sujet des données d'être informé de cette collecte et des traitements subséquents auxquels les données collectées seront soumises si ces données sont collectées exclusivement auprès de tiers.

Outre les informations qui doivent être fournies au sujet des données en vertu de la proposition de directive, la Commission désire, par ailleurs, que soient également désignés au sujet des données les tiers ou catégories de tiers auxquels les données le concernant seront éventuellement communiquées.

En ce qui concerne l'article 9, 2, la Commission accepte la dérogation apportée par la première phrase ("dans le cas visé à l'article 8, § 1, (b)").

Elle considère que la deuxième phrase de ce paragraphe devrait être modifiée dans le sens suivant afin de tenir compte de la nécessité d'informer le sujet des données au moment de la **collecte** des données et non à celui de leur communication : "l'obligation d'informer n'existe pas dans le cas où le **traitement** est imposé par la loi".

Quant au paragraphe 3, la Commission est satisfaite que le responsable du fichier soit tenu de cesser le traitement à l'encontre duquel le sujet des données émet des objections.

Elle souhaite cependant faire deux observations sur la manière dont le texte est rédigé pour l'instant.

Premièrement, elle estime que cette obligation devrait être étendue au traitement effectué grâce au fichier, que ce traitement soit effectué par le responsable du fichier lui-même ou par une autre personne. Le responsable du fichier devrait, dès lors, être tenu de cesser ou de faire cesser le traitement en cause.

Deuxièmement, elle considère que la dérogation exprimée par les termes "sauf si une disposition légale l'y autorise" est trop large. Elle souhaiterait son remplacement par les mots suivants : "sauf si une disposition légale l'y oblige ou l'y autorise expressément".

Article 10 (exceptions particulières à l'obligation d'informer la personne concernée).

L'article 10 permet aux Etats membres de prévoir dans leur législation que l'autorité de contrôle peut autoriser une dérogation à l'obligation d'informer la personne concernée dans quatre types de circonstances :

-"lorsque l'information de la personne concernée se révèle impossible" : pas d'objection;

-"lorsque l'information de la personne concernée implique des efforts disproportionnés" : la Commission se demande par rapport à quoi les efforts doivent être disproportionnés; elle craint que des raisons économiques ne soient trop souvent

invoquées pour se soustraire à l'obligation d'informer la personne concernée; elle souhaiterait à tout le moins que le mot "disproportionnés" soit remplacé par "déraisonnables";

-"lorsque l'information de la personne concernée se heurte à des intérêts légitimes prédominants du responsable du fichier" : la Commission ne peut accepter cette exception particulière que parce qu'il appartiendra à l'autorité de contrôle d'apprécier, dans les cas d'espèce, si les intérêts légitimes prédominants du responsable du fichier justifient réellement l'exception;

-"lorsque l'information de la personne concernée se heurte à un intérêt similaire d'un tiers" : la Commission ne peut accepter cette exception que pour la même raison. Elle souhaite, afin d'éviter tout risque de confusion, qu'à l'expression "un intérêt similaire d'un tiers" soit substituée celle de "les intérêts légitimes prédominants d'un tiers".

La Commission prend note que, selon les précisions données dans l'exposé des motifs, l'autorité de contrôle peut préciser les conditions de la dérogation et décider d'informer elle-même le sujet des données.

Article 11 (notification à l'autorité de contrôle).

La Commission approuve entièrement l'obligation de notification à l'autorité de contrôle de l'établissement d'un fichier de données à caractère personnel.

Elle regrette, par contre, à nouveau que cette obligation soit circonscrite aux seuls cas dans lesquels les données du fichier sont destinées à être communiquées.

Elle considère que, pour exercer un contrôle efficace du respect des mesures imposées en matière de protection des données, l'autorité de contrôle doit avoir connaissance de tous les fichiers constitués - du moins de tous les fichiers susceptibles de faire l'objet de traitements automatisés, y compris par le recours au scanning - même si les données qu'ils contiennent ne sont initialement pas destinées à être communiquées.

La Commission se demande, de plus, pourquoi les fichiers dont les données sont destinées à faire l'objet de consultations en ligne ne sont, cette fois, pas visés.

La Commission admet, au contraire, la dérogation en faveur des fichiers dont les données proviennent de sources généralement accessibles au public pour autant que ces fichiers ne contiennent pas aussi d'autres données à caractère personnel. Une précision en ce sens à l'article 11, 1, lui semble nécessaire.

Par ailleurs, elle juge favorablement l'obligation de nouvelle notification en cas de changement de finalité du fichier ou de changement d'adresse.

La Commission n'a pas d'objection à l'égard des paragraphes 2 et 3. Elle estime néanmoins que le paragraphe 3 devrait permettre également aux Etats d'imposer également soit la déclaration de destruction d'un fichier, soit une déclaration périodique de poursuite de l'utilisation d'un fichier afin que le registre tenu par l'autorité de contrôle puisse être mis à jour en éliminant les mentions relatives aux fichiers qui auraient cessé d'exister.

CHAPITRE IV - DROITS DE LA PERSONNE CONCERNEE

Article 12 (consentement informé).

L'article 12 définit la notion de consentement au sens où elle est mentionnée dans la proposition de directive.

La Commission constate avec satisfaction que cette définition, qui correspond à celle généralement admise du "consentement éclairé", la précise de manière particulièrement utile.

Outre l'information qui doit être délivrée au sujet des données, la Commission approuve particulièrement les précisions relatives à l'objet et à la forme du consentement, ainsi que la faculté de **retrait** du consentement pour l'avenir prévue au paragraphe 3.

Article 13 (information lors de la collecte).

La Commission approuve le principe de l'article 13.

Elle estime néanmoins que la rédaction du texte est perfectible car le fait que cet article n'est applicable qu'en cas de collecte de données auprès de la personne concernée par ces données elle-même ne ressort qu'indirectement de son texte[18] alors que cette limitation apparaît plus clairement dans l'exposé des motifs.

La Commission estime également que, puisque l'article 13, 1, n'est pas destiné à s'appliquer lors de la collecte de données auprès de tiers par rapport au sujet des données, cette hypothèse devrait aussi être réglée dans une autre disposition, qui imposerait de fournir à ces tiers certaines informations, c'est-à-dire celles reprises aux litteras (a) à (d), avant qu'ils ne fournissent les informations.

Même un tiers par rapport au sujet des données peut, en effet, être prêt à fournir ces données dans certaines circonstances et pas dans d'autres.

La Commission estime, en principe, acceptables les dérogations apportées au principe d'information par le paragraphe 2. Elle propose toutefois qu'il soit précisé qu'il doit s'agir de "cas prévus par la loi".

Article 14 (droits complémentaires de la personne concernée).

L'article 14 dresse un catalogue des droits du sujet des données.

La Commission ne peut évidemment qu'approuver entièrement la reconnaissance de ces droits par la proposition de directive.

Elle souhaite néanmoins exprimer quelques observations sur cette importante disposition.

L'article 14, 1, accorde au sujet des données le droit de s'opposer, **pour des raisons**

[18] Au paragraphe 1, (c), et (e).

légitimes, à ce que des données à caractère personnel le concernant fassent l'objet d'un traitement.

Selon l'exposé des motifs, les "raisons légitimes" doivent être interprétées dans le sens étroit où un traitement de données ne remplit pas les conditions imposées par ou en vertu de la directive en projet, notamment en ce qui concerne sa légitimité.

La Commission peut accepter cette interprétation étroite, mais elle tient à mettre en évidence qu'elle rend d'autant plus indispensable que les critères et conditions établis par la proposition de directive soient les plus précis, les plus stricts et les plus protecteurs possibles.

Les critiques et suggestions émises dans cet avis en prennent d'autant plus d'importance.

La Commission marque son accord avec le droit cité à l'article 14, 2, mais, en raison des divergences qui existent quant au concept de profil de personnalité, elle propose que soient insérés les mots "même partielle" à la 4ème ligne, entre les termes "définition" et "du profil", afin que ce droit ne se voie pas attribuer une portée trop limitée.

La Commission approuve sans commentaire particulier le droit établi par l'article 14, 3, qui est inspiré par la législation existant dans plusieurs Etats de la Communauté européenne.

La Commission approuve également le droit reconnu à l'article 14, 4.

Bien qu'elle approuve également le droit visé à l'article 14, 5, elle émet certaines craintes quant à la possibilité d'obtenir le "**verrouillage**" des données. Il ressort de l'exposé des motifs que cette possibilité porte sur le cas dans lequel des données exactes font l'objet de traitements qui violent les dispositions de la proposition de directive. Les données peuvent être conservées dans le fichier, mais elles ne peuvent plus être utilisées.

La Commission estime qu'il devrait être précisé expressément dans le texte de la disposition même que le verrouillage ne concerne que cette hypothèse.

Elle ne peut, par ailleurs, accepter que le verrouillage vise également les données qui ont été **collectées** en violation de la directive proposée, comme l'indique l'exposé des motifs. Si les données ont été collectées en violation de certains principes de la directive, elles ne peuvent être conservées dans le fichier; elles doivent être effacées.

Les droits prévus aux paragraphes 4, 6, 7 et 8 font l'objet de l'approbation sans réserve de la part de la Commission.
Celle-ci tient, en particulier, à souligner l'importance du recours juridictionnel accordé au sujet des données au paragraphe 8.

Article 15 (exceptions au droit d'accès aux fichiers du secteur public).

L'article 15 détermine les limites du droit établi par l'article 14, 3 et 4, en ce qui concerne les fichiers du secteur public.

La Commission n'a pas d'objection envers les exceptions prévues aux litteras (a), (b) et (c).

Elle est, au contraire, très réservée à l'égard de l'exception qui serait justifiée par la sécurité publique (littera d), telle que cette dernière est définie dans l'exposé des motifs ("toutes les fonctions de police des organes de l'Etat, y compris la **prévention** de la criminalité").

En effet, les fonctions de police comprennent tant les tâches accomplies dans le cadre de missions de police judiciaire que de **police administrative**. Sont donc également visées les activités policières accomplies en l'absence de toute infraction. Ceci est d'ailleurs confirmé par la précision "y compris la prévention de la criminalité" dans l'exposé des motifs.

Ainsi interprétée, cette exception pourrait avoir une portée très large.

La Commission est parfaitement consciente que les impératifs des investigations policières peuvent, même en matière de prévention, imposer que la personne suspecte ne soit pas informée des informations dont disposent les organes de police à son sujet. Elle estime toutefois que seule l'existence de soupçons sérieux est de nature à justifier pareille exception au droit d'accès.

Indépendamment du contrôle prévu à l'article 15, 2, la Commission recommande dès lors que le littera (d) soit complété par les mots "dans les cas où les données du fichier font peser des soupçons sérieux sur la personne concernée".

La Commission n'a pas d'observation particulière sur l'article 15, 1, (d).

Elle s'interroge sur la portée à attribuer à l'expression de "nécessité de l'exercice des fonctions de contrôle ou d'inspection de l'autorité publique", (littera f), qui n'est pas définie, et elle se demande dans quelle mesure cette "nécessité" peut réellement justifier une exception au droit d'accès de la personne concernée.

Elle considère, en outre, que le refus d'accès qui serait ainsi justifié ne devrait être, en toutes circonstances, que temporaire.

La Commission est opposée à l'exception prévue à l'article 15, 1, (g).

Si, comme le précise l'exposé des motifs, celle-ci vise, entre autres, la protection d'intérêts tels que les secrets commerciaux d'autres parties, la Commission se demande pourquoi il serait impossible d'extraire d'un ensemble de données celles qui se rapportent seulement à la personne qui exerce son droit d'accès sans divulguer les données relatives à d'autres personnes ou sans divulguer que certaines des données fournies se rapportent aussi à d'autres personnes.

Quant à l'autre exemple cité par l'exposé des motifs, celui de la liberté de la presse, la Commission constate que, puisque l'article 15 ne concerne que les fichiers publics, il établirait une discrimination, en ce qui concerne la liberté de la presse, entre les organes de presse relevant du secteur public (agences de presse officielles, réseaux de radiodiffusion et de télévision publics ...) et les organes de presse privés.

En outre, l'exception prévue à l'article 15, 1, (g), ne vise pas le traitement des données,

ce qui entraverait effectivement la mise en oeuvre de la liberté de la presse, mais seulement l'accès aux données de la personne concernée. Or, le droit d'accès lui paraît être une garantie raisonnable à accorder à la personne concernée lorsque le droit à la protection des données à caractère personnel et la liberté de la presse entrent en conflit et qu'un équilibre doit, par conséquent, être recherché entre ces deux droits fondamentaux.

La Commission approuve entièrement l'article 15, 2, selon lequel, lorsque est invoqué un des motifs relatifs à la sécurité publique pour refuser le droit d'accès du sujet des données, l'autorité de contrôle dispose, elle, du droit d'accès aux données litigieuses et elle peut apprécier, en fonction des circonstances et du contenu des données, si le refus du droit d'accès est, ou non, légitime.

Enfin, la Commission ne s'oppose pas à l'exception établie par l'article 15, 3, mais elle souhaite que celle-ci soit mieux définie : en l'état actuel du texte, le droit d'accès aux données visées pourrait être refusé pendant des décennies.

Elle propose, dès lors, que ce paragraphe soit rédigé de la manière suivante :

"les Etats membres peuvent limiter, pendant un délai maximal d'un an, le droit d'accès de la personne concernée aux données compilées temporairement sous la forme de données à caractère personnel afin d'en extraire des informations statistiques et destinées à être rendues anonymes".

Article 16 (qualité des données).

La Commission approuve entièrement cet article, dont le paragraphe 1 reproduit presque textuellement l'article 5 de la Convention n° 108 du Conseil de l'Europe.

Il s'agit d'un article très important.

La Commission apprécie, en outre, positivement que soit désignée - au paragraphe 2 - une personne à qui incombe de faire observer les principes énoncés, personne qui pourrait, en cas de non-respect de ces principes, faire l'objet des sanctions établies en vertu de l'article 23 de la proposition de directive. Elle souhaiterait que cette disposition soit également applicable au gestionnaire du fichier.

Article 17 (catégories particulières de données).

L'article 17 porte sur le traitement de ce qu'il est désormais convenu d'appeler les "données sensibles". Il reprend les catégories de données énumérées à l'article 6 de la Convention du Conseil de l'Europe, en remplaçant toutefois l'expression "autres convictions" par celle de "convictions philosophiques" et en créant les deux catégories précises d'"opinion politique" et d'"appartenance syndicale". Il faut également noter que la catégorie des données révélant l'origine raciale a été complétée par la mention de l'origine ethnique, ce qui devrait éviter toute hésitation quant à l'interprétation à donner à cette catégorie de données.

L'article 17 érige un principe plus protecteur que la Convention du Conseil de l'Europe puisqu'il **interdit**, en principe, le traitement des données sensibles autres que les condamnations pénales et qu'il réserve la conservation des données portant sur ces dernières aux fichiers du secteur public.

La Commission constate avec beaucoup de satisfaction l'extension de la protection ainsi accordée. Elle craint cependant que la dérogation au principe de l'interdiction de traitement prévue au paragraphe 1 en cas d'accord du sujet des données ne prenne trop d'importance en pratique.

Aussi recommande-t-elle, en premier lieu, que cette dérogation ne soit pas fondée sur l'accord, mais sur le "consentement informé" de la personne concernée.

Elle recommande, en second lieu, que le traitement de données sensibles ne puisse avoir lieu, même si le sujet des données y a consenti, que dans des cas prévus par la loi.

En outre, elle considère que l'interdiction de principe du traitement de données sensibles ne doit plus être limitée au traitement automatisé, mais qu'elle doit désormais porter également sur le traitement manuel.

Elle suggère par conséquent, de reformuler l'article 17, 1, de la manière suivante :

"Les Etats membres interdisent le traitement des données révélant l'origine raciale et ethnique, l'opinion politique, les convictions religieuses ou philosophiques, les appartenances syndicales ainsi que les informations relatives à la santé et à la vie sexuelle d'une personne.

Les Etats membres peuvent toutefois autoriser le traitement de certaines de ces données dans les cas prévus par la loi lorsqu'il est rendu nécessaire par les droits, libertés ou intérêts de la personne concernée et que celle-ci a donné son consentement libre, exprès et écrit à ce traitement".

Le troisième paragraphe du commentaire de l'exposé des motifs relatif à l'article 17 pourrait être complété de manière à citer, à titre d'exemple, que les cas dans lesquels les droits, libertés ou intérêts de la personne concernée rendent le traitement de catégories particulières de données nécessaires visent, entre autres, les libertés d'association et d'expression et la préservation de la bonne santé physique et psychique de la personne concernée.

La Commission accepte la dérogation, prévue au paragraphe 2, au traitement de données sensibles.

La Commission émet un avis très positif sur la précision que les dérogations doivent être faites sur base d'une loi et que cette loi doit prévoir les garanties appropriées contre les utilisations abusives et les accès non autorisés. Enfin, la Commission a une opinion favorable à l'égard de la **conservation** des données concernant les condamnations pénales dans les seuls fichiers relevant du secteur public imposée au paragraphe 3.

Article 18 (sécurité des données).

L'article 18 de la proposition de directive impose une obligation importante au responsable du fichier qui, au-delà du respect par lui-même des principes de protection des données, doit prendre toutes les mesures techniques et d'organisation appropriées pour faire respecter ces principes par tous.

La Commission salue cette initiative et relève avec satisfaction que le responsable du fichier devra, à cet égard, tenir compte du plan d'action relatif à la sécurité informatique qui

sera élaboré par la Commission européenne sur base de l'article 29 de la loi.

Elle regrette néanmoins que l'article 18, 1, alinéa 2, restreigne les mesures que doit prendre le responsable du fichier en fonction du "coût de leur mise en oeuvre".

Elle considère, dès lors, que celui-ci doit supporter le coût - même important - des mesures qui s'imposent en l'état de l'art en la matière afin de réduire l'intensité du risque qu'il crée - par la constitution du fichier - à son profit.

CHAPITRE V - DISPOSITIONS SPECIFIQUES POUR CERTAINS SECTEURS

Article 19 (liberté de la presse).

La Commission considère aussi que, comme le prévoit ce principe, des dérogations aux principes contenus dans la proposition de directive doivent être admises lorsque la protection des données à caractère personnel entre en conflit avec un autre droit fondamental, à savoir la liberté de la presse.

Elle considère toutefois que l'article 19 ne suffit pas pour résoudre ce problème complexe. Il faudrait prendre en considération divers critères tels que le fait qu'une personne physique ait, ou non, une vie publique ou qu'elle s'en soit retirée, le fait qu'elle ait commis un acte délictueux et les évaluer en fonction de différents principes tels que, par exemple, la présomption d'innocence.

Elle suggère, dès lors, que l'examen de cette question soit poursuivi au niveau communautaire ou, mieux, à un niveau plus large, sur base des travaux du Conseil de l'Europe en la matière, de manière à élaborer, à l'avenir, des recommandations à ce propos qui fournissent aux Etats membres des indications leur permettant d'adapter leur droit en fonction de l'article 19 dans un sens commun.

La Commission souhaite également attirer l'attention sur la nécessité que certaines organisations privées internationales à caractère humanitaire, telles qu'Amnesty International et la Croix-Rouge internationale, doivent pouvoir également bénéficier, dans des limites et conditions strictement définies, de dérogations aux principes protecteurs déterminés dans la proposition de directive, dans la mesure où cela est indispensable, aux principes régissant les catégories particulières de données.

Article 20 (codes de conduite sectoriels).

La Commission partage le souci exprimé dans la proposition de directive par la Commission européenne d'encourager divers milieux professionnels à se doter de codes de conduite sectoriels - ou d'entreprise - en matière de protection des données à caractère personnel.

La Commission considère néanmoins, qu'afin de tenir compte des traditions de chaque Etat membre, ces codes de conduite devraient être élaborés dans le respect des normes juridiques existantes ou à définir.

Elle propose dès lors de faire commencer l'article 19 par les mots suivants : "sans

préjudice des normes sectorielles communautaires[19] et des dispositions juridiques internes sectorielles".

Il faudrait, en outre, préciser que les codes de conduite sectoriels doivent être soumis à l'approbation de l'autorité de contrôle.

CHAPITRE VI - RESPONSABILITE ET SANCTIONS

Article 21 (responsabilité).

L'article 21 de la proposition de directive tend à imputer au responsable du fichier la responsabilité civile pour tout dommage subi par une personne du fait du traitement ou de toute action incompatibles avec les dispositions de la directive.

La Commission émet un avis favorable sur cette disposition, mais elle tient à exprimer les considérations suivantes.

Tout d'abord, elle considère que, du fait de la désignation d'une personne - le responsable du fichier - présumée responsable quel que soit l'auteur du traitement ou de l'action incompatible avec la directive en projet, l'article 21 établit une responsabilité **objective**.

La responsabilité du responsable du fichier sera donc engagée même si l'auteur du fait dommageable est un tiers.

La Commission se prononce favorablement à l'établissement d'une responsabilité objective en ce domaine, qui est de nature à alléger la charge de la preuve que doit apporter la victime - le sujet des données - et à lui permettre de déterminer aisément contre qui elle doit diriger son action judiciaire - sans devoir rechercher l'éventuel auteur d'un traitement dommageable particulier.

Elle souhaite cependant que le responsable du fichier puisse, du point de vue de la contribution à la dette, introduire un recours contre le véritable auteur du fait dommageable et elle suggère de compléter l'article 21, 1, en ce sens.

La Commission peut, d'autre part, accepter le renversement de la charge de la preuve résultant du paragraphe 2 au sujet des causes d'exonération fondées sur les article 18 et 22. Elle tient à insister sur l'importance d'une révision de l'article 18, 1, alinéa 2, dans le sens qu'elle a suggéré, puisque le respect de cette disposition constitue une cause d'exonération de responsabilité sur base de l'article 21, 2.

La Commission présume par ailleurs, que la victime d'un dommage résultant d'un traitement ou d'une action **compatible** avec les dispositions de la directive proposée ou survenu en dépit du respect des articles 18 et 22 conserve, nonobstant l'article 21, 1 et 2, le droit d'agir en justice contre l'auteur d'une **faute** au regard du **droit commun**.

[19] L'exposé des motifs précise que la Commission européenne tiendra compte des initiatives des milieux professionnels dans l'exercice de son pouvoir réglementaire ou pour faire de nouvelles propositions.

Article 22 (traitement pour le compte du responsable du fichier).

La Commission considère que l'article 22 devrait faire expressément référence à la notion de gestionnaire du fichier.

Elle s'étonne, par ailleurs, de constater qu'alors que des dispositions régissent les traitements de données réalisés par le responsable du fichier et pour son compte, aucune disposition ne porte spécifiquement sur les traitements effectués par des tiers grâce aux données d'un fichier avec l'autorisation du maître du fichier, sans que ces traitements soient effectués pour le compte de ce dernier.

Elle considère que les dispositions proposées qui se rapportent à la légitimité du traitement et à la communication ou à la consultation en ligne ne règlent que partiellement le traitement effectué par un tiers grâce aux données du fichier[20].

Article 23 (sanctions).

La Commission est satisfaite que la proposition de directive impose aux Etats membres d'appliquer des sanctions afin d'assurer le respect des dispositions prises en vertu de cette directive.

Elle souhaiterait néanmoins qu'il y soit précisé que les sanctions doivent être prises tant à l'égard du "responsable du fichier" qu'à l'égard de tout autre utilisateur des données, y compris le gestionnaire du fichier.

La Commission est d'avis que, même dans les cas où le "responsable du fichier" est une personne morale, le caractère dissuasif exigé par l'article 23, implique que des sanctions pénales sont prévues à l'égard des personnes physiques.

CHAPITRE VII - TRANSFERT DE DONNEES VERS DES PAYS TIERS

Article 24 (principes).

L'article 24 est supposé régir les flux transfrontières de données à caractère personnel des Etats membres de la Communauté européenne vers les pays tiers.

Le principe fondamental à cet égard est énoncé au paragraphe 1 : "le transfert ... ne peut avoir lieu que si (le pays tiers) assure un niveau de protection **adéquat"**.

Qu'est-ce qu'un "niveau de protection adéquat" ? L'exposé des motifs ne fournit pas la moindre indication à ce propos.

Pourtant, la répétition dans quatre des cinq paragraphes de l'article 24 de l'expression "niveau de protection adéquat" confère à celle-ci une importance particulière.

---

[20] Voy. d'ailleurs les critiques exprimées envers ces dispositions dans la mesure où elles concernent des tiers par rapport au "responsable du fichier".

Il faut remarquer que c'est en définitive, selon l'article 24, 3 et 4, à la Commission européenne qu'il appartiendra de déterminer si un pays tiers offre un "niveau de protection adéquat".

Le paragraphe 3 prévoit que la Commission européenne peut engager des négociations avec le pays tiers qui ne dispose pas d'un niveau de protection "adéquat" et dont la situation résultant de cette absence de niveau de protection adéquat est préjudiciable aux intérêts de la Communauté ou d'un Etat membre.

Il ne suffit donc pas qu'un pays tiers ne dispose pas du niveau de protection adéquat pour engager des négociations; il faut, en outre, que la situation qui en résulte soit préjudiciable aux intérêts de la Communauté européenne ou de l'un de ses Etats membres.

L'intérêt des sujets des données semble tout à fait oublié.

Le paragraphe 4 accorde à la Commission européenne le pouvoir de décider, après **avis** du Comité consultatif composé par les représentants des **Etats** membres - et non des autorités de contrôle! - qu'un pays tiers assure un niveau de protection adéquat en raison des engagements internationaux qu'il a souscrits ou de sa législation interne.

L'avis du Comité consultatif ne lie pas la Commission européenne. C'est, par conséquent, elle seule qui est véritablement compétente pour décider qu'un pays tiers assure un niveau de protection adéquat.

La décision qu'elle rend sur le niveau de protection adéquat n'est apparemment fondée que sur les engagements internationaux et la législation interne du pays tiers sans prendre en considération la pratique interne de ce pays.

La synthèse de l'article 24, 1 à 4, de la directive en projet fait donc apparaître que le transfert - temporaire ou définitif - de données vers un pays tiers ne peut avoir lieu que si ce pays assure un "niveau de protection adéquat", c'est-à-dire indéfini, qui est apprécié par la Commission européenne et elle seule en ne tenant compte que des engagements internationaux et de la législation interne du pays tiers considéré, quelle que soit sa pratique interne. Si des négociations sont entamées avec le pays tiers, elles le sont sur base d'une décision de la Commission européenne - à nouveau - fondée non seulement sur le niveau de protection inadéquat, mais aussi sur la condition supplémentaire que ce niveau inadéquat soit à l'origine d'une situation préjudiciable aux intérêts de la Communauté ou de l'un de ses Etats membres, quel que soit le préjudice subi par les sujets des données.

Enfin, le paragraphe 5, particulièrement obscur, dispose que "les mesures prises au titre (de l'article 24) sont conformes aux obligations qui incombent à la Communauté en vertu d'accords internationaux tant bilatéraux que multilatéraux qui régissent la protection des données ..."

L'exposé des motifs n'apporte aucun éclaircissement sur cette disposition, qui semble impliquer que les décisions prises par la Commission peuvent violer les garanties très théoriques proclamées à l'article 24, 1 à 4, pour autant que ces décisions soient prises conformément aux obligations souscrites par la Communauté dans le cadre d'accords internationaux.

Cet article 24, 5, peut être utilisé de la meilleure comme de la pire façon, selon la nature des engagements internationaux qui seront souscrits - sur base de quels critères ? - et de l'interprétation que leur prêtera la Commission européenne.

La Commission considère que l'ensemble de l'article 24 est absolument inacceptable.

Elle considère que l'article 24 devrait, en tout état de cause, viser, comme la Convention du Conseil de l'Europe, la notion de "protection équivalente" à la place de celle, indéfinissable, de porter de "protection adéquate".

Elle estime, par ailleurs, que la proposition de directive devrait prévoir le verrouillage des données destinées à être transmises dans un pays tiers dans l'attente d'avoir déterminé si ce pays tiers offre effectivement un niveau de protection équivalent des données à caractère personnel.

Article 25 (dérogations à l'article 24).

Cet article a pour but d'autoriser, de manière ponctuelle, le transfert de données vers un pays tiers qui n'offre pas un niveau de protection "adéquat, à condition que le responsable du fichier - soumis à la directive en projet - présente des garanties suffisantes".

La Commission approuve l'idée sous-jacente de cette disposition, mais elle estime qu'elle devrait être traduite avec une plus grande précision.

Cette disposition s'inspire, en fait, de la technique dite "des clauses contractuelles".

Aussi la Commission préférerait-elle que l'article proposé précise expressément que le responsable du fichier doit présenter l'engagement contractuel du destinataire des données de prendre des mesures assurant à ces données un niveau de protection équivalent à celui dont elles bénéficient dans le fichier d'origine et de permettre le contrôle pratique de l'efficacité de ces mesures par le responsable du fichier.

CHAPITRE VIII - AUTORITE DE CONTROLE ET GROUPE DE PROTECTION DES DONNEES

Article 26 (autorité de contrôle).

L'article 26 impose aux Etats membres qui n'en disposent pas encore de mettre en place une autorité de contrôle indépendante chargée de surveiller l'application des dispositions relatives à la protection des données à caractère personnel, à laquelle soient conférés des pouvoirs d'investigation et d'intervention.

La Commission approuve totalement cette obligation imposée aux Etats membres.

Article 27 (groupe de protection des données).

L'article 27 institue un groupe de protection des données à caractère personnel au niveau communautaire, constitué de représentants des autorités de contrôle des Etats membres et présidé par un représentant de la Commission européenne. Ce groupe de

protection des données a un **caractère consultatif** auprès de la Commission européenne.

La Commission est extrêmement favorable à la constitution d'une autorité de contrôle à l'échelle de la Communauté européenne.

Elle regrette de devoir émettre de vives critiques à l'égard de la proposition faite par la Commission européenne à ce sujet.

En ce qui concerne la composition du groupe de protection des données, elle approuve la représentation en son sein des autorités de contrôle des Etats. Elle ne comprend toutefois pas pourquoi la Commission européenne devrait être représentée au sein de ce groupe, ni, à fortiori, pourquoi elle devrait en assurer la présidence.

Elle préférerait que le président soit **élu** par les membres du groupe et qu'il soit choisi parmi eux.

Article 28 (mission du Groupe de protection des données).

L'article 28 définit les missions du Groupe de protection des données.

La Commission constate que la description de ces missions est répartie sur trois paragraphes dont certaines dispositions semblent se chevaucher. Elle estime, en outre, que certaines compétences, notamment celles visées à l'article 28, 1a, et 2, sont décrites d'une façon trop timide.

Elle suggère, dès lors, de remplacer les paragraphes 1 à 3 par le paragraphe suivant:

"1. Le Groupe de protection des données à caractère personnel a pour mission:

a.de donner des avis, à la demande de la Commission, sur l'application de la présente directive dans les Etats membres, sur le niveau de protection dans la Communauté et dans les pays tiers, et sur des projets de mesures à prendre dans le domaine de la protection de la vie privée;

b.d'émettre d'initiative des recommandations sur toute question concernant la protection des personnes à l'égard des données à caractère personnel dans la Communauté.

Les avis et les recommandations sont inscrits au procès-verbal et peuvent être transmis au Comité consultatif visé à l'article 30. La Commission informe le Groupe de protection des données à caractère personnel des suites qu'elle a données aux avis et recommandations."

L'article 28, 4, prévoit l'établissement d'un rapport annuel par le Groupe de protection des données. La Commission accueille favorablement cette idée. Elle souhaite, en outre, que le rapport soit publié ou, à tout le moins, que le Groupe soit habilité à communiquer son rapport, en plus de la Commission européenne, à toute personne qu'il juge utile.

CHAPITRE IX - POUVOIR REGLEMENTAIRE DE LA COMMISSION

Article 29 (exercice du pouvoir réglementaire).

La Commission n'a pas d'objection de principe à ce que la Commission européenne arrête les modalités d'application de la directive.

Elle suggère toutefois, quant à la procédure à suivre, que la Commission européenne soit tenue de demander l'avis, non seulement du Comité consultatif (article 30), mais aussi du Groupe de protection des données à caractère personnel.

Article 30 (Comité consultatif).

L'article 30 établit un Comité consultatif composé des représentants des Etats membres.

La Commission estime qu'il n'y a pas lieu, pour elle, de formuler des observations sur cette disposition.

III - Appréciation globale de la proposition de directive

1)La Commission considère que la proposition de directive relative à la protection des personnes à l'égard du traitement des données à caractère personnel est destinée à répondre à un besoin réel et actuel: celui d'assurer un haut niveau de protection des données à caractère personnel dans l'ensemble des Etats membres et d'harmoniser les dispositions légales, réglementaires et administratives des Etats membres afin que le même haut niveau de protection soit maintenu lorsque des données sont communiquées entre des entités établies dans des Etats membres différents.

La Commission doit malheureusement constater que ces objectifs ne sont pas entièrement atteints par le texte proposé.

2) En premier lieu, le champ d'application de la directive est trop limité.

Cette limitation du champ d'application résulte, certes, en partie de la limite même des compétences qui sont attribuées au Conseil en vertu du Traité de Rome. La Commission est, à ce propos, très satisfaite que la Commission européenne ait proposé, en même temps que la directive qui fait l'objet du présent avis, un projet de résolution des représentants des gouvernements des Etats membres des Communautés européennes destinée à étendre l'application des principes contenus dans la directive au secteur public ne relevant pas du champ d'application du droit communautaire.

Le champ d'application de la directive est, par contre, limité sciemment du fait de sa détermination par référence aux fichiers, même si des dispositions particulières se rapportent également à certaines formes de traitement des données.

Il est également limité par l'article 4, qui exclut les fichiers localisés dans des pays tiers et dont l'utilisation par une personne qui réside sur le territoire d'un Etat membre n'est que

sporadique.

3) En second lieu, les conditions requises pour qu'un traitement de données - tant dans le secteur public que dans le secteur privé - ou de certains types de traitements particuliers de données, tels que leur communication, sont souvent beaucoup trop larges et accroissent, par ce fait même, le nombre et la diversité des traitements dont les données peuvent faire l'objet.

Le laxisme de certaines de ces conditions porte aussi une atteinte très sérieuse au principe fondamental du respect des finalités.

4) Des principes très positifs sont introduits dans la proposition de directive, mais ils sont le plus souvent affaiblis par les exceptions et dérogations qui y sont acceptées.

Tel est, en particulier, le cas en ce qui concerne l'information de la personne concernée, la modification de l'établissement d'un fichier de données à caractère personnel, et les différents droits complémentaires de la personne concernée.

IV - Conclusion

Eu égard aux observations qui précèdent, la Commission ne peut qu'émettre un avis défavorable au texte actuel de la proposition de directive.

Le Secrétaire,	Le Président,
A. PIPERS	D. HOLSTERS