NATIONS UNIES **E**

Conseil économique et social

Distr.
GENERALE

E/CN.4/1995/75
23 décembre 1994

FRANCAIS
Original : ANGLAIS/FRANCAIS/ESPAGNOL

COMMISSION DES DROITS DE L'HOMME

Cinquante et unième session
Point 14 de l'ordre du jour

DROITS DE L'HOMME ET PROGRES DE LA SCIENCE ET DE LA TECHNIQUE

Question du suivi des principes directeurs pour la réglementation des fichiers personnels informatisés

Rapport du Secrétaire général établi conformément à la décision 1993/113 de la Commission

TABLE DES MATIERES

TABLE DES MATIERES (suite)

Introduction

1. Dans sa décision 1993/113 du 10 mars 1993, la Commission des droits de l'homme, se référant aux principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (E/CN.4/1990/72) adoptés par l'Assemblée générale dans sa résolution 45/95 du 14 décembre 1990, a décidé de demander au Secrétaire général de lui faire rapport à sa cinquante et unième session :

a) Sur l'application des principes directeurs au sein du système des Nations Unies ;

b) Sur les informations recueillies auprès des Etats et des organisations intergouvernementales, régionales et non gouvernementales concernant le suivi des principes directeurs sur les plans régional et national.

2. Conformément à cette décision, le 4 mai 1994, le Secrétaire général a demandé aux organes, organismes et institutions spécialisées des Nations Unies de lui communiquer des informations sur l'application des principes directeurs dans les secvices concernés du système des Nations Unies.

3. A la même date, des demandes ont également été envoyées aux Etats et aux organisations intergouvernementales et non gouvernementales pour recueillir des informations touchant le suivi desdits principes directeurs sur les plans régional et national.

4. A la date du 1er décembre 1994, le Secrétariat avait reçu des réponses des organes, organismes et institutions spécialisées des Nations Unies indiqués ci-après : Département de la coordination des politiques et du développement durable, Fonds des Nations Unies pour les activités en matière de population, Université des Nations Unies, Cour internationale de Justice, Programme alimentaire mondial, Organisation des Nations Unies pour l'alimentation et l'agriculture, Organisation mondiale de la santé, Organisation maritime internationale, Agence internationale de l'énergie atomique.

5. Des informations ont été communiquées par les gouvernements des pays suivants : Allemagne, Arabie saoudite, Argentine, Croatie, Espagne, Luxembourg, Malte, Norvège, Philippines, République centrafricaine, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Suède, Yougoslavie.

6. Ont également envoyé des réponses les organisations intergouvernementales ci-après : Commission africaine des droits de l'homme et des peuples, Conseil de l'Europe, Interpol.

7. Aucune réponse n'a été reçue des organisations non gouvernementales.

8. On trouvera dans le présent rapport un résumé des réponses contenant des informations concrètes. Les réponses qui pourraient être reçues ultérieurement feront l'objet d'additifs au présent document.

I. APPLICATION DES PRINCIPES DIRECTEURS AU SEIN DU SYSTEME DES NATIONS UNIES

9. Sur les 62 organes, organismes, commissions régionales, institutions spécialisées et organisations relevant des Nations Unies auxquels des demandes ont été adressées, 10 seulement ont répondu*.

10. Le Département de la coordination des politiques et du développement durable et l'Université des Nations Unies ont indiqué qu'ils n'avaient aucune information à communiquer sur l'application des principes directeurs touchant les fichiers personnels informatisés.

11. La Cour internationale de Justice a répondu qu'elle ne pouvait donner aucune information à ce sujet étant donné qu'elle n'utilisait pas encore de fichiers informatisés.

12. L'Organisation maritime internationale (OMI) a indiqué qu'elle souscrivait aux principes directeurs en question et prendrait des dispositions pour les faire appliquer lorsqu'elle informatiserait les fichiers personnels à usage interne.

13. L'Agence internationale de l'énergie atomique a fait savoir que le Statut et le Règlement du personnel de l'AIEA ainsi que les mesures et procédures en vigueur pour la collecte, la gestion et la protection des données à caractère personnel informatisées ou autres étaient conformes aux principes directeurs énoncés dans le document E/CN.4/1990/72.

14. Le Fonds des Nations Unies pour les activités en matière de population a aussi indiqué qu'il respectait toutes les garanties énoncées dans les principes directeurs.

15. L'Organisation des Nations Unies pour l'alimentation et l'agriculture ainsi que le Programme alimentaire mondial ont répondu que le système informatisé de fichiers contenant des données à caractère personnel de la FAO était utilisé essentiellement par le service de la paie, c'est-à-dire pour l'attribution automatique des indemnités et prestations liées aux traitements. Les données personnelles en question concernaient seulement la nationalité, le sexe, la date de naissance et l'état civil, sans indication de race, de religion, de groupe ethnique, etc. Ces fichiers étaient exclusivement à usage interne. Les données à caractère personnel n'étaient communiquées aux tiers qu'avec l'accord du fonctionnaire concerné. Un sous-système de sécurité avait été mis en place pour protéger les fichiers contre tout accès non autorisé et abusif. Il était précisé que la FAO respectait les grands principes énoncés dans la partie A du document E/CN.4/1990/72.

16. L'Organisation internationale du Travail (OIT) a fait savoir que le Département du Personnel du BIT connaissait depuis deux ans au moins les Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Lorsque le BIT a décidé d'utiliser le Système intégré de gestion (SIG) de l'ONU comme base de son nouveau Système d'information sur le personnel et les états de paie (PERSIS), il

---

* Les textes peuvent être consultés au Secrétariat.

s'est renseigné sur les principes directeurs dont une description détaillée se trouve dans le "Conditions of Work Digest" du BIT, Volume 10, 2/1991.

17. L'OIT a été invitée à une réunion sur la protection des données à caractère personnel, organisée en octobre 1993 sous l'égide du Conseil de l'Europe, au cours de laquelle l'accent a été mis sur la manière dont les organisations internationales réglaient la question. Toutes les organisations présentes à la réunion ont fait le point et exposé leurs problèmes. Ce fut pour l'OIT une seconde occasion de se pencher sur la question.

18. Le Département du personnel a examiné le texte des Principes directeurs et y souscrit totalement. Toutefois, le principe 9 n'est pas applicable à l'OIT.

19. L'OIT (BIT), dont le nouveau système d'information sur le personnel est fondé sur le Système intégré de gestion (SIG) de l'ONU, suppose que celui-ci a été construit en appliquant les Principes directeurs des Nations Unies. A en juger par l'examen effectué par le BIT des données qui seront mises en mémoire dans sa propre version du SIG (PERSIS), aucune d'entre elles ne pourrait être considérée comme non conforme aux Principes directeurs.

20. Les problèmes qui se poseront à l'OIT (BIT) concerneront l'exactitude, spécialement eu égard à l'obligation de mise à jour, car il est très coûteux de passer continuellement en revue les données pour que les informations nouvelles soient mises en mémoire dès qu'elles sont connues. Le BIT a l'intention de mettre au point un "document-navette" qui serait distribué à tous les fonctionnaires et indiquerait la liste des données importantes qui figurent dans leur fichier nominatif. Les fonctionnaires seront invités à vérifier l'exactitude des données et à les mettre à jour, puis à renvoyer le document au Département du personnel qui les traitera. Cette procédure permet de satisfaire aux exigences des principes 2 et 4.

21. En ce qui concerne les fichiers non informatisés, l'OIT (BIT) a jugé les Principes directeurs acceptables également. Le BIT avait auparavant un système comportant deux fichiers personnels manuels (A et B), le fonctionnaire n'ayant pas accès au fichier B. Ce système est en cours de modification. Aucun nouveau fichier B n'est constitué; les anciens sont en cours de traitement et seront rendus accessibles prochainement à chaque fonctionnaire concerné.

22. Il n'y a pas à l'OIT (BIT) de personne spécifiquement chargée de contrôler le respect des principes en question. Bien que l'OIT ait élaboré des conventions et des recommandations sur la question des données à caractère personnel, elle n'a pas encore adopté ses propres principes pour réglementer la gestion des données en question au sein du BIT.

23. En outre, le Service des conditions de travail et des activités de bien-être du BIT a publié deux nouveaux volumes du "Conditions of Work Digest" qui abordent aussi certains aspects du traitement des fichiers informatisés.

24. L'Organisation mondiale de la santé (OMS) a communiqué les informations ci-après :

Budget et finances

25. Tous les fichiers personnels de ce secteur sont confidentiels à la base. Le Système d'information administrative et financière (AFI) de l'OMS fonctionne sur une base sélective, celle de la "nécessité d'accès".

Gestion du système d'information

26. A l'OMS, le système d'information est géré par la Division de la gestion du système d'information (ISM). Cette division développe certaines applications informatiques, mais il s'agit de systèmes d'information communs ou d'entreprise, c'est-à-dire destinés à l'usage de l'ensemble des programmes ou des divisions de l'OMS, par opposition aux systèmes uniques utilisés par une seule unité organisationnelle. A cet égard, il n'existe pas de systèmes d'information communs contenant des fichiers de données à caractère personnel autres que celles figurant dans l'élément Personnel du Système AFI que gère la Division du budget et des finances et, selon notre interprétation des Principes directeurs, les données en question ne sont pas considérées comme des données ipso facto à caractère personnel.

27. La Division de la gestion du système d'information aide les programmes ou les divisions à trouver des consultants pour élaborer les systèmes uniques dont ils ont besoin. A notre connaissance, les programmes et les divisions n'ont pas de systèmes uniques contenant des données à caractère personnel autres que celles de l'élément Personnel mentionné plus haut.

Personnel

28. Les fichiers personnels de la Division du Personnel sont gérés conformément aux principes directeurs énoncés dans le document E/CN.4/1990/72 de l'ONU.

II. INFORMATIONS COMMUNIQUEES PAR DES ETATS

A. Argentine

[Original : espagnol]
[12 octobre 1994]

29. La Convention nationale constituante, qui a commencé ses travaux de réforme de la Constitution argentine le 25 mai 1994, a adopté le 22 août 1994 un texte entré en vigueur le 24 août de la même année en vertu duquel un nouveau chapitre était ajouté à la Première Partie de la Constitution sous le titre de "Garanties et droits nouveaux". L'article 43 dudit texte consacre au niveau constitutionnel le recours en protection déjà prévu au niveau législatif, et dispose ce qui suit au paragraphe 3 :

> "Toute personne peut former ce recours en vue de prendre connaissance des données la concernant contenues dans des registres ou banques de données publics ou privés destinés à l'élaboration de rapports, de connaître leur finalité et, en cas d'erreur ou de discrimination, en vue d'en exiger la suppression, la rectification, le classement comme confidentielles ou la mise à jour. Il ne peut être porté atteinte au secret des sources d'information des journalistes".

De cette manière, le recours en "habeas data" est expressément reconnu dans une norme constitutionnelle.

B. République centrafricaine

[Original : français]
[13 juillet 1994]

30. Le Gouvernement de la République centrafricaine est pour sa part décidé à tout mettre en oeuvre pour assurer le respect des principes directeurs dont il s'agit, en les intégrant à ses législation et réglementation nationales en la matière. C'est dans ce sens que toutes les administrations de la République centrafricaine ont reçu copie du document E/CN.4/1990/72 relatif à ces principes directeurs aux fins d'en tenir compte.

C. Croatie

[Original : anglais]
[1er septembre 1994]

31. Dans la République de Croatie, les données à caractère personnel concernant l'état civil (registre des naissances, des mariages et des décès, registre de la nationalité, et listes électorales) sont enregistrées sur ordinateur dans la plupart des localités; il y a toutefois des localités où ces registres sont encore tenus manuellement.

32. Il incombe au Ministère de l'administration de superviser les organes de l'administration publique qui établissent les listes électorales et tiennent les

registres d'état civil (naissances, mariages, décès). Les listes électorales sont des registres officiels contenant la liste des citoyens jouissant du droit de vote. Dans les registres d'état civil sont consignées les données requises par la loi concernant la naissance, le mariage et le décès.

33. Les registres de nationalité sont tenus par les organes de l'administration publique - bureaux de l'administration générale, placés sous la tutelle administrative du Ministère de l'administration; en revanche, l'application des dispositions relatives à la nationalité et aux registres de nationalité relèvent de la compétence du Ministère de l'Intérieur.

34. Le Ministère de la défense dresse la liste des appelés conformément à la loi sur la défense. La République de Croatie est en train d'informatiser tout le système des registres d'appelés.

35. Les listes électorales et registres d'état civil, en République de Croatie, ne sont pas reliés à un système informatique central. L'informatisation de ces données s'est effectuée en partie dans les services de l'administration publique directement chargés de les tenir et à ce jour, ces données n'ont pas été raccordées entre elles sur le territoire de la République de Croatie. Leur raccordement à un système central reste encore à faire, mais cela dépendra de considérations financières.

36. Les données à caractère personnel concernant le droit de vote et l'état civil sont recueillies, traitées et utilisées conformément aux Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (E/CN.4/1990/72). La réglementation de la République de Croatie énonçant les procédures à suivre pour tenir les registres en question reprend les principes en question :

a) Les données à recueillir sont stipulées par la loi, de même que la manière dont elles sont traitées et l'usage auquel elles sont destinées (Principe de licéité);

b) Une loi séparée dispose qu'il incombe aux organes de l'administration publique de vérifier l'exactitude et la pertinence des données (Principe d'exactitude);

c) L'usage auquel sont destinées les données recueillies est stipulé par la loi qui précise à quelles fins elles peuvent être utilisées et dans quelles circonstances. Par exemple, le fait d'être inscrite dans les registres officiels confère à une personne le droit d'obtenir des documents permettant de prouver des faits relatifs à la naissance, au mariage ou au décès. Les services de l'état civil délivrent plusieurs types de documents (extraits, actes de naissance, pièces d'état civil) qui constituent une preuve de données à caractère personnel, selon les besoins et la demande (Principe de finalité);

d) Les données relatives au droit de vote sont accessibles au public pendant les élections alors que les données à caractère personnel (naissance, mariage, décès) font l'objet d'une protection spéciale touchant à la fois l'accès aux registres officiels et l'obtention de documents officiels. Les documents officiels sont délivrés à la demande d'une personne qui a un intérêt au regard de la loi, alors que l'accès aux registres d'état civil est autorisé à la personne à laquelle se rapportent les données en question, aux membres de sa

famille directe, à ses parents adoptifs ou à son gardien/sa gardienne et à d'autres personnes à condition qu'elles aient un intérêt légitime stipulé par la loi (Principe de l'accès par la personne concernée);

e) Les registres susmentionnés ne contiennent pas de données sur l'origine raciale ou religieuse, la couleur, la vie sexuelle, les idées politiques, religieuses, philosophiques ou autres ni sur l'affiliation à une association ou un syndicat, de sorte qu'elles ne peuvent servir de base à une discrimination quelconque fondée sur l'un des critères que l'on vient de mentionner (Principe de non-discrimination);

f) La loi ne prévoit pas la possibilité d'utiliser les données à des fins exceptionnelles susceptibles de violer les principes énoncés aux alinéas a) à e) ci-dessus.

37. Il existe des dispositions spéciales sur la sécurité des données. Les listes électorales doivent être conservées pendant cinq ans à compter de la date à laquelle elles sont arrêtées (elles le sont immédiatement avant les élections) tandis que les registres d'état civil (naissances, mariages, décès) sont conservés en permanence.

38. Les données informatisées sont protégées de la destruction et de la dégradation par une procédure spéciale consistant à faire des copies et à les stocker en lieu sûr.

39. Malheureusement, en dépit de toutes les mesures de sécurité, la République de Croatie n'a pas accès aux registres concernant les territoires provisoirement occupés. On ignore si les données à caractère personnel concernant les citoyens ont été détruites.

40. Les mesures de sécurité concernant le traitement informatique visant à protéger les données à caractère personnel contre tout usage non autorisé sont les suivantes : un signe spécial de programme pour chaque travail; des postes de saisie pour un seul travail (données accessibles seulement aux personnes autorisées); un certain programme se voit attribuer seulement la structure de données correspondante. Néanmoins, la République de Croatie n'a toujours pas de législation sur la sécurité des systèmes d'information concernant à la fois les mesures de protection matérielle et des programmes. Les mesures de protection des programmes des systèmes d'information exigent des programmes spéciaux de protection des données qui puissent assurer l'intégrité totale d'une banque de données et commencer à fonctionner immédiatement en cas de panne du système pour quelque raison que ce soit.

41. C'est le Ministère de l'administration qui contrôle l'application de la loi concernant les registres d'état civil (naissances, mariages, décès) et les listes électorales et il appartient au Ministère de l'Intérieur de contrôler l'application de la loi organique concernant le registre de nationalité.

42. La loi sur la protection des données à caractère personnel est en cours d'élaboration et devrait être adoptée fin 1994. Elle prévoira un mécanisme de protection juridique de tous les groupes structurés de données à caractère personnel (pas seulement informatisées).

43. La loi envisagée est fondée sur les principes énoncés dans les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'Organisation de coopération et de développement économiques (Paris, 1980) et dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe, Strasbourg, 1981). Ces principes étant également contenus dans les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, le projet de loi contient déjà les principes des numéros 1 à 9.

44. Cette loi a pour objectif primordial d'assurer la protection des données à caractère personnel (des citoyens auxquels les données se rapportent) et d'établir à cet effet les droits, principes, procédures et conditions relatifs à la prévention des immixtions non autorisées, irrégulières et non nécessaires (excessives) dans la vie privée à l'occasion de toutes les activités de collecte, de traitement, de stockage et d'utilisation des données à caractère personnel dans la sphère publique et privée.

D. Allemagne

[Original : anglais]
[9 août 1994]

45. Comme beaucoup d'autres Etats européens, la République fédérale d'Allemagne et ses Länder fédéraux ont adopté des lois sur la protection des données dans leurs domaines de compétence respectifs. En 1970, le Land fédéral de Hesse a été le premier au monde à se doter d'une loi sur la protection des données; la première loi fédérale sur la protection des données (Bundesdatenschutzgesetz, BDSG) a été adoptée en 1977. Il existe des lois sur la protection des données dans tous les Länder, dont certaines sont déjà des lois de la deuxième ou troisième génération. La loi fédérale (BDSG) aussi a été entièrement modifiée en 1990.

46. En raison du partage des compétences établi par la Loi fondamentale (Grundgesetz), la BDSG ou loi fédérale réglemente la protection des données dans les organes publics fédéraux ainsi que dans les organismes privés, tandis que les lois sur la protection des données des Länder contiennent des dispositions réglementant cette protection dans les organes publics du Land concerné. Certaines lois sectorielles, comme le Code du droit social, comportent aussi des dispositions sectorielles de protection des données.

47. De surcroît, la protection des données est consacrée par la Constitution allemande. La Cour constitutionnelle fédérale (Bundesverfassungsgericht), dans son arrêt concernant la loi sur le recensement (Volkszählungsgesetz) du 15 décembre 1983, a reconnu que les droits généraux à la liberté énoncés au paragraphe 1 de l'article 2 de la Constitution, lu dans le contexte du paragraphe 1 de l'article 1er de la Constitution, englobent le "droit pour l'individu de déterminer l'usage et la divulgation des données le ou la concernant". Les limitations de ce droit sont autorisées seulement dans la mesure où l'intérêt public est prépondérant et elles sont énoncées dans une loi clairement définie qui respecte le principe du caractère raisonnable.

48. La législation allemande sur la protection des données anticipait plus ou moins les principes directeurs élaborés par les Nations Unies. Il n'a donc pas été vraiment nécessaire de les incorporer au droit allemand en adoptant une loi.

49. Les informations fournies ci-dessous, avec une référence à chacun des principes directeurs de l'ONU, concernent la loi fédérale ou BDSG. Mais on retrouve une réglementation parallèle dans les lois sur la protection des données des Länder.

a) Principe 1 - La loi allemande sur la protection des données interdit l'utilisation des données à caractère personnel sauf disposition contraire de la loi ou consentement de la personne faisant l'objet des données (article 4, subdivision 1 de la loi fédérale BDSG);

b) Principe 2 - Tout responsable du contrôle des fichiers est tenu d'assurer la protection des données à caractère personnel en prenant des mesures d'ordre technique et organisationnel (article 9 de la BDSG);

c) Principe 3 - Dans "l'arrêt sur le recensement" mentionné plus haut, la Cour constitutionnelle fédérale a déjà établi les principes de finalité et d'utilisation des données conformément aux fins spécifiées. Ces principes ont été pris en compte à l'article 14 de la BDSG, pour n'en citer qu'un, lequel donne une liste exhaustive des faits qui, pour des raisons importantes, justifient l'utilisation des données à des fins autres que celles qui ont été spécifiées (par ex. poursuites pénales, prévention d'un danger);

d) Principe 4 - La loi allemande sur la protection des données accorde à la personne concernée le droit d'accès aux données (articles 19, 34 de la BDSG) ainsi que le droit d'obtenir la rectification, la destruction et le blocage (articles 20, 35 de la BDSG). Aux termes de l'article 6 de la BDSG, ces droits font partie des droits de la personne fichée qui sont d'application obligatoire, c'est-à-dire qui ne peuvent faire l'objet de forclusion ni de restriction même avec l'accord de la personne concernée (article 6 de la BDSG);

e) Principe 5 - La protection spéciale des données sensibles est principalement réglementée dans les lois sectorielles;

f) Principe 6 - Les critères énoncés dans ce principe reflètent fidèlement la teneur des lois et de la Constitution allemandes. Le droit pour l'individu de déterminer l'utilisation qui peut être faite des données le concernant doit constamment être mis en balance avec d'autres garanties constitutionnelles et peut parfois être supplanté par des droits d'une valeur supérieure ou équivalente;

g) Principe 7 - L'article 9 de la BDSG fait obligation à tous ceux qui contrôlent les fichiers de prendre des mesures d'ordre technique et organisationnel afin de garantir l'intégrité des données à caractère personnel. Une liste en dix points contenant des instructions très concrètes figure en annexe à cet article;

h) Principe 8 - Dans les organismes publics de la Fédération et des Länder, le respect des dispositions relatives à la protection des données relève du Commissaire fédéral à la protection des données et des Commissaires à la protection des données des Länder. Ces commissaires exercent leurs fonctions de

manière indépendante et ne sont soumis qu'à la loi et aux règlements professionnels, comme les juges. Pour les entités privées, c'est-à-dire essentiellement les sociétés privées, le contrôle est exercé par les autorités de supervision du Land, qui doivent appliquer des instructions et font partie de la hiérarchie administrative. Ces autorités sont en revanche indépendantes de l'organisme qu'elles contrôlent, comme l'exige le Principe 8. Dans la mesure où le droit pénal général (par exemple, les articles 201 et suivants du Code pénal) ne s'applique pas en cas d'infraction aux dispositions relatives à la protection des données, la BDSG (article 43, 44) et les lois de chaque Land sur la protection des données qualifient certains cas spéciaux d'infraction au règlement ou d'infraction pénale;

i) Principe 9 - La République fédérale appuie et applique le principe des "garanties comparables" lorsque des données sont communiquées hors frontières. Lors de l'élaboration des dispositions législatives pertinentes, il convient de mettre en balance le niveau de protection offert par le pays récipiendaire et les intérêts de la personne concernée par les données;

j) Principe 10 - La BDSG s'applique aux fichiers manuels et informatisés et, dans le domaine public, s'applique aussi aux registres, c'est-à-dire à tout document établi à des fins officielles. Toutefois, le champ d'application de la BDSG n'englobe pas les personnes morales. Mais la protection des données concernant les personnes morales, qui sont presque exclusivement des sociétés, découle du principe de la liberté des échanges consacré à l'article 12 de la Constitution. En Allemagne, la protection des données en question relève du domaine du droit commercial au sens large, et non du droit relatif à la protection des données.

E. Luxembourg

[Original : français]
[16 septembre 1994]

50. Le Luxembourg dispose, depuis 1979, d'une loi réglementant l'utilisation des données nominatives dans les traitements informatiques, modifiée par la suite*, répondant aux "Principes directeurs pour la réglementation des fichiers personnels informatisés" (E/CN.4/1990/72), adoptés par l'Assemblée générale dans sa résolution 45/95 du 14 décembre 1990.

51. Par la loi du 19 novembre 1987, le Luxembourg a approuvé la Convention (du Conseil de l'Europe) pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg, le 28 janvier 1981 (STE 108), seul instrument juridique international contraignant existant à ce jour.

---

* Les textes peuvent être consultés au Secrétariat.

F. Malte

[Original : anglais]
[3 octobre 1994]

52. Le Gouvernement maltais a indiqué que tous les points couverts par les Principes directeurs (E/CN.4/1990/72) étaient traités dans le projet de législation générale actuellement examiné par le Cabinet avant d'être soumis pour adoption à la Chambre des représentants de Malte. Cette loi, intitulée Loi sur les pratiques informatiques (Information Practices Act), devrait entrer en vigueur à la mi-1995.

G. Norvège

[Original : anglais]
[23 août 1994]

53. Le Gouvernement norvégien a mentionné dans sa réponse la Loi sur les fichiers de données personnelles (Personal Data Register Act, PDRA) du 9 juin 1978* ainsi que les règlements édictés en application de cette loi le 21 décembre 1978 et les amendements du 10 mars 1981*, dans lesquels les principes directeurs énoncés dans le document E/CN.4/1990/72 étaient pris en compte de la manière suivante :

a) Le principe 1 était pris en compte dans la loi du 9 juin 1978 ainsi que, dans la pratique, par l'Inspection des données établie en vertu de cette loi;

b) Le principe 2 était pris en compte à l'article 8 de la loi du 9 juin 1978;

c) Le principe 3 était pris en compte au paragraphe 1 de l'article 11 de la loi du 9 juin 1978, par l'Inspection des données, dans la pratique, ainsi que par les Règlements édictés en vertu des articles 1-2, paragraphe 2, de la loi;

d) Le principe 4 était pris en compte à l'article 7 de la loi du 9 juin 1978;

e) Le principe 5 était pris en compte à l'article 6, paragraphe 2, de la loi du 9 juin 1978;

f) Le principe 6 était pris en compte aux articles 9 et 6 de la loi du 9 juin 1978;

g) Le principe 7 était pris en compte aux articles 8 b) et 11 de la loi du 9 juin 1978 et dans la pratique, par l'Inspection des données;

h) Le principe 8 était pris en compte aux articles 2, 5 et 38 de la loi du 9 juin 1978;

---

* Les textes peuvent être consultés au Secrétariat.

i) Le principe 9 était pris en compte à l'article 36 de la loi du 9 juin 1978 et au chapitre 8 des Règlements;

j) Le principe 10 était pris en compte aux articles 1 et 9 de la loi du 9 juin 1978.

H. Philippines

[Original : anglais]
[22 septembre 1994]

54. Le Gouvernement philippin a fait savoir qu'il avait institué certaines normes ou garanties, dont témoignaient plusieurs lois et cas faisant jurisprudence, parmi lesquels notamment :

a) Dispositions législatives :

i) La Constitution des Philippines, à l'article III, section 3(1), dispose que "le secret des communications et de la correspondance ne sera pas violé sauf sur décision des tribunaux prise conformément à la loi";

ii) La loi 4200 de la République, dite "Loi anti-écoutes téléphoniques", interdit et punit l'utilisation d'un dispositif électronique pour intercepter toute communication en vue d'obtenir des informations au sujet d'une personne donnée;

iii) Le Code civil philippin, en son article 32, punit tout fonctionnaire ou employé de l'Etat ou tout particulier qui, directement ou indirectement, fait obstacle ou porte atteinte au caractère privé des communications ou de la correspondance;

iv) Les Mémorandums-Circulaires nos 78 et 196 (de la Présidence) promulguent les règles qui régissent la sécurité des questions classées confidentielles dans les services officiels, interdisent la divulgation d'informations figurant dans des documents officiels et font obligation aux services administratifs concernés d'inscrire la mention "Confidentiel" sur les documents ayant ce caractère, avec l'avertissement suivant :

> " La divulgation non autorisée d'informations figurant dans les documents ci-joints, sans compromettre la sécurité nationale, serait préjudiciable aux intérêts ou au prestige de la nation, ou à tout autre activité officielle, ou risque de causer des embarras d'ordre administratif, de porter un tort injustifié à un particulier ou d'avantager une nation étrangère";

v) Le Code pénal révisé, en son article 228, punit tout fonctionnaire public qui, sans y être dûment habilité, ouvre ou autorise l'ouverture de tous documents, papiers ou objets clos confiés à sa garde. A l'article 229, le Code pénal révisé punit

tout fonctionnaire public qui révèle un secret quelconque connu de lui en raison de ses fonctions officielles ou délivre à tort des documents relevant de sa responsabilité. L'article 230 dudit Code sanctionne tout fonctionnaire public qui divulgue des secrets concernant un particulier dont il a eu connaissance dans le cadre de ses fonctions;

b) Jurisprudence philippine :

i) Dans l'affaire Valmonte c. Belmonte Jr. (170 SCRA 256) la Cour suprême des Philippines a statué le 13 février 1989 que "il ne peut y avoir aucun doute sur le fait que le droit à la vie privée est protégé par la Constitution";

ii) Dans l'affaire Orfe c. Mutuc (130 Phil 415, 1968 et 22 SCRA 424), qui a fait date, la Cour suprême des Philippines, s'exprimant par la voix du juge Fernando, a déclaré :

> "Le droit à la vie privée en tant que tel est reconnu, indépendamment de son assimilation à la liberté, comme méritant pleinement la protection de la Constitution. Les propos du Pr. Emerson sont particulièrement pertinents en l'occurrence : 'La notion de pouvoir gouvernemental limité a toujours impliqué l'idée d'un gouvernement dont les pouvoirs s'arrêtaient en-deçà de certaines intrusions dans la vie privée du citoyen. C'est d'ailleurs l'une des distinctions fondamentales qui existent entre le pouvoir absolu et le pouvoir limité. Le contrôle total et envahissant de l'individu, dans tous les domaines de la vie, est la marque du pouvoir absolu. Au contraire, le régime de gouvernement à pouvoir limité préserve une sphère privée qui appartient à l'individu, et qu'il distingue bien de la sphère publique que l'Etat peut contrôler. La protection de cette sphère privée - qui est, en d'autres termes, la protection de la dignité et de l'intégrité de l'individu - revêt de plus en plus d'importance avec le développement de la société moderne. Toutes les forces à l'oeuvre dans l'ère technologique - l'industrialisation, l'urbanisation et l'organisation - tendent à rétrécir la sphère privée et à faciliter l'intrusion dans cette sphère. Aujourd'hui, c'est la capacité à préserver et à défendre cette enclave de la vie privée qui marque la différence entre société démocratique et société totalitaire.'"

55. Les Philippines estiment que les dispositions législatives et la jurisprudence mentionnées plus haut sont des garanties suffisantes pour renforcer le droit de la personne à la vie privée. Il s'agit de normes essentielles pour consolider le droit à la détermination individuelle tel qu'il est envisagé dans les Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel. Lorsque ces Principes directeurs auront été vraiment adoptés comme moyens d'atteindre les objectifs visés par la législation et la jurisprudence philippines susmentionnées, ils favoriseront et renforceront l'intégrité des

droits fondamentaux des Philippines dans la mesure où ils vont se fondre avec ceux de toute la communauté humaine.

56. Par conséquent, les Philippines ne voient aucune raison de ne pas appuyer la version révisée des Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel établie par les Nations Unies. C'est pour cette raison et dans cet esprit que la Commission philippine des droits de l'homme a adopté les Principes directeurs pour l'utilisation et la gestion des fichiers informatisés contenant des données à caractère personnel*.

I. Arabie saoudite

[Original : anglais]
[30 mai 1994]

57. Le Gouvernement de l'Arabie saoudite a communiqué les observations suivantes :

> " Les "fichiers informatisés contenant des données à caractère personnel" sur les citoyens sont la propriété de l'Etat. Par conséquent, les "Principes directeurs" concernant ce dispositif ne s'appliquent pas à l'Arabie saoudite".

J. Espagne

[Original : espagnol]
[15 juillet 1994]

58. Le Gouvernement espagnol a communiqué les textes législatifs suivants :

a) Loi organique 5/1992 du 29 octobre 1992, portant réglementation du traitement automatisé des données à caractère personnel (Journal officiel espagnol du 31 octobre 1992)*;

b) Décret royal 428/1993 du 26 mars 1993, portant approbation des Statuts de l'Agence de protection des données*;

c) Décret royal 1332/1994 du 20 juin 1994, développant des aspects spécifiques de la Loi organique 5/1992 du 29 octobre 1992 portant réglementation du traitement automatisé des données à caractère personnel*.

---

* Les textes peuvent être consultés au Secrétariat.

K. Suède

[Original : anglais]
[25 août 1994]

59. Le Gouvernement suédois a indiqué que la Suède protégeait depuis longtemps la vie privée à l'égard des fichiers informatisés contenant des données à caractère personnel. La loi suédoise sur la protection des données de 1973 a été la première loi nationale de son espèce dans le monde. (Le texte de la loi, telle qu'elle a été modifiée à compter du 1er juillet 1992, était joint en annexe)*. En 1982, la Suède a été le premier pays à ratifier la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ETS 108).

60. La loi de 1973 réglemente l'utilisation des fichiers contenant des données à caractère personnel, c'est-à-dire les fichiers, listes et autres notes qui font l'objet d'un traitement automatique des données et qui contiennent des données à caractère personnel concernant une personne physique identifiable. Les fichiers manuels n'entrent pas dans le champ d'application de la loi de 1973.

61. La Loi de 1973 stipule qu'il faut un responsable du contrôle de chaque fichier automatisé contenant des données à caractère personnel. Le contrôleur du fichier est la personne physique ou morale ou l'organisme qui décide des informations devant figurer dans le fichier et peut, si besoin est, modifier le fichier ou en transformer le contenu pour le rendre lisible.

62. Aux termes des dispositions de la loi de 1973 sur la protection des données, quiconque souhaite constituer un fichier automatisé de données à caractère personnel est tenu d'en informer l'Agence suédoise de protection des données (Datainspektionen) et d'obtenir une licence à cet effet. Cette licence donne au contrôleur du fichier le droit de créer et d'exploiter un nombre illimité de fichiers se rapportant à la licence spécifique obtenue.

63. Outre l'obligation d'obtenir une licence, la loi de 1973 contient des dispositions applicables à certains fichiers contenant des données sensibles, pour lesquels une autorisation spéciale de l'Agence est requise. Parmi les catégories spéciales de données à caractère personnel qui font l'objet d'une protection particulière figurent les données sur les condamnations pénales ou les internements administratifs, les données concernant la santé ou la vie sexuelle ou révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres. Une autorisation est également requise pour mettre en oeuvre des fichiers contenant des mentions restrictives sur les personnes. Il faut aussi obtenir une autorisation pour les fichiers contenant des informations sur des personnes sans lien direct avec le contrôleur. S'il existe un lien spécial entre le contrôleur du fichier et la personne dont les données sont enregistrées, les fichiers sont exonérés de l'obligation d'autorisation. C'est le cas par exemple des fichiers contenant des informations sur des usagers, clients, membres d'une organisation, etc ou sur des employés. Pour le "croisement" des fichiers, c'est-à-dire le transfert de données d'un fichier à l'autre et le traitement groupé de plusieurs fichiers contenant des données à caractère personnel, il faut aussi l'autorisation de l'Agence.

---

* Les textes peuvent être consultés au Secrétariat.

64. L'Agence de protection des données peut accorder son autorisation seulement s'il n'y a aucune raison de penser que le traitement automatique des données à caractère personnel du fichier risque d'empiéter indûment sur le droit au respect de la vie privée de la personne fichée.

65. Il faut aussi l'autorisation de l'Agence pour transférer un fichier dans un autre pays, sauf s'il s'agit d'un pays signataire de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel de 1981. L'Agence peut donner son autorisation seulement si elle peut considérer que le transfert ne va pas porter atteinte au droit de la personne fichée au respect de sa vie privée.

66. Il y a aussi certaines dispositions générales sur le stockage des fichiers de données à caractère personnel dans les archives.

67. L'Agence de protection des données supervise les contrôleurs de fichiers ainsi que l'application générale de la Loi.

68. Si le traitement automatique des données a porté atteinte ou si l'on peut craindre qu'il ne porte indûment atteinte au droit à la vie privée, l'Agence peut fixer des conditions spécifiques pour le traitement automatique des données ou, s'il n'est pas possible de réviser le contenu du fichier en procédant autrement, interdire au contrôleur d'exploiter le fichier ou encore retirer l'autorisation accordée antérieurement.

69. Les décisions de l'Agence de protection des données sont susceptibles d'appel devant le gouvernement.

70. En 1993, une Commission a soumis une proposition de loi nouvelle sur la protection des données. Vu l'incertitude qui règne sur le point de savoir quel sera à l'avenir le niveau de protection des données en Europe, le gouvernement a décidé de ne pas présenter de proposition de loi nouvelle pour le moment.

71. En attendant, le 14 avril 1994, le gouvernement a présenté au Parlement un projet de loi avec des amendements à la Loi de 1973 sur la protection des données visant à restreindre le système des autorisations spéciales et à élargir le rôle de supervision de l'Agence de protection des données. Entre autres dispositions, le projet de loi contient aussi une proposition aux termes de laquelle les décisions de l'Agence de protection des données seraient susceptibles d'appel devant une instance judiciaire et non plus devant le gouvernement comme c'est le cas actuellement. Il est envisagé que les amendements à la Loi sur la protection des données entrent en vigueur le 1er janvier 1995.

L. Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

[Original : anglais]
[15 septembre 1994]

72. Le gouvernement a indiqué que la législation britannique sur la protection des données prenait en compte les principes généraux énoncés dans les Principes directeurs des Nations Unies. La Loi de 1984 sur la protection des données confère des droits aux personnes faisant l'objet de données traitées par

informatique (c'est-à-dire sur ordinateur). Le particulier en question peut demander quelles sont les informations détenues à son sujet, en contester l'exactitude et, dans certains cas, exiger une réparation. Les détenteurs de données à caractère personnel informatisées doivent être inscrits au Registre de la protection des données (Data Protection Registrar), et respecter des règles spécifiques sur la manière dont ils obtiennent, enregistrent et utilisent leurs données.

73. Les éléments clés de la Loi de 1984 sont les suivants :

a) La Loi s'applique à toutes les données à caractère personnel qui sont informatisées ou sous une forme se prêtant au traitement automatisé, sauf les données traitées à domicile en vue d'un usage personnel ou celles traitées par les sociétés pour les états de paie, les pensions, la comptabilité, les achats ou les ventes (mais pas les dossiers concernant le personnel ou la commercialisation). Il y a aussi des exceptions lorsque l'information est destinée uniquement à la diffusion d'articles ou d'informations auprès des personnes fichées par des clubs dotés de la personnalité morale, pour les données que l'utilisateur est tenu par la Loi de rendre publiques (par ex. les listes électorales), ou lorsque les données sont détenues pour des raisons de sécurité nationale (déterminées par les ministres du gouvernement);

b) Tous les utilisateurs de données qui ne sont pas dispensés de cette obligation doivent déclarer le type de données qu'ils détiennent, les utilisations auxquelles les données sont destinées, les sources d'où émanent ces données, les personnes auxquelles les données peuvent être divulguées et tout pays étranger à destination duquel les données peuvent être transférées;

c) Les utilisateurs de données doivent se conformer aux principes régissant la protection des données. Selon ces principes, les données à caractère personnel doivent être recueillies et traitées selon des procédés loyaux et licites, être détenues seulement à des fins licites déclarées et consignées dans le registre, être utilisées à ces seules fins et être divulguées seulement aux personnes indiquées dans la déclaration consignée sur le registre. Les données doivent être adéquates, pertinentes et ne pas outrepasser les limites de leur finalité, être exactes et, le cas échéant, mises à jour; elles ne doivent pas être conservées plus longtemps qu'il n'est nécessaire pour les fins déclarées lors de l'inscription et être entourées de toutes les mesures de sécurité requises;

d) Le directeur du Registre peut adresser trois types d'avis pour assurer le respect desdits principes : un avis de mise en demeure spécifiant les mesures à prendre, un avis d'annulation de l'inscription supprimant la totalité ou une partie de la déclaration consignée au registre (constitue un délit la détention de données non couvertes par une déclaration consignées au registre) et un avis d'interdiction de transfert à l'étranger;

e) Les sujets fichés (les personnes physiques, non les organisations) peuvent demander une réparation en justice pour les dommages causés par la perte, la destruction ou la divulgation non autorisées de données à caractère personnel ou pour le tort causé par des données inexactes. La personne fichée peut aussi porter plainte auprès du directeur du Registre ou s'adresser aux tribunaux pour réclamer le rectification ou la suppression des données. Elle peut aussi, moyennant une demande écrite et le paiement d'une redevance, se

procurer auprès d'un utilisateur des données une copie des informations à caractère personnel la concernant (sauf par exemple, dans les cas où l'accès de cette personne fichée à ces données risquerait de compromettre la prévention ou la détection d'un crime). La personne concernée peut déposer plainte auprès du directeur du Registre ou s'adresser aux tribunaux pour obtenir une injonction si l'accès ne lui a pas été accordé dans un délai de 40 jours;

f) Une personne fichée qui considère qu'il y a eu violation de l'un des principes ou de l'une des dispositions de la Loi peut porter plainte auprès du directeur du Registre, qui doit instruire la plainte si elle est sérieuse et présentée sans retard excessif. Le directeur du Registre peut chercher à régler l'affaire par la voie officieuse, engager des poursuites ou émettre une mise en demeure à l'encontre d'un utilisateur de données;

g) Un utilisateur de données peut divulguer des informations concernant un particulier, à condition que la destination des données ait été correctement indiquée dans l'inscription au registre ou qu'il y ait "exemption de non-divulgation" (par exemple, si la divulgation est requise par la loi ou faite avec l'accord de la personne fichée);

h) Le directeur du Registre fait rapport directement au Parlement. Il tient le Registre des utilisateurs de données et des centres de traitement à façon, le met à la disposition du public et diffuse des informations sur la Loi et son fonctionnement. Le directeur du Registre encourage aussi le respect des principes et, le cas échéant, favorise l'élaboration de codes d'usages. Il examine les plaintes pour violation des principe énoncés dans la Loi et, le cas échéant, engage des poursuites ou émet des mises en demeure;

i) Les utilisateurs de données ou centres de traitement à façon peuvent faire appel des décisions du directeur du Registre devant un tribunal de la protection des données en cas de refus d'enregistrer des demandes d'inscription, avis de mise en demeure, retrait d'inscription ou avis d'interdiction de transfert. Le tribunal peur renverser la décision du directeur du Registre. Les points de droit peuvent faire l'objet d'un nouvel appel devant un tribunal de première instance.

74. Des exemplaires de certaines instructions élaborées par le directeur du Registre de la protection des données, avec des explications détaillées de la Loi de 1984, ont été joints par le Gouvernement britannique*.

M. Yougoslavie

[Original : anglais]
[14 novembre 1994]

75. Le Gouvernement de la République fédérative de Yougoslavie a communiqué les informations reproduites dans les paragraphes qui suivent.

76. La huitième session des deux Conseils de l'Assemblée fédérale, qui s'est tenue le 2 octobre 1990, a adopté la Loi portant ratification de la Convention

---

* Les textes peuvent être consultés au Secrétariat.

pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Ce faisant, la République fédérative de Yougoslavie a contracté l'obligation de réglementer, dans sa législation interne, la question de la protection des données à caractère personnel contenues dans les fichiers informatisés.

77. Sur la base du paragraphe 4 de l'article 33 de la Constitution de la République fédérative de Yougoslavie, aux termes duquel la loi fédérale réglemente la collecte, le traitement, l'utilisation et la protection des données à caractère personnel, le Ministère fédéral des droits de l'homme et des minorités et l'Institut fédéral d'informatique ont rédigé un projet de loi sur la protection des données à caractère personnel qui a été approuvé à la 164ème séance du gouvernement fédéral, le 21 avril 1994. Les dispositions du projet de loi sont conformes à celles de la Convention précitée. Le projet de loi est maintenant en cours d'examen par l'Assemblée fédérale.

78. Le projet de loi sur la protection des données à caractère personnel contient tous les principes figurant dans les Principe directeurs, excepté en ce qui concerne le statut des fichiers contenant des données à caractère personnel détenus par les organisations internationales gouvernementales. Les principes directeurs qui sont repris dans ce projet de loi sont indiqués ci-dessous :

a) Principe de licéité et de loyauté : articles 1 et 2 du projet de loi;

b) Principe d'exactitude : article 12 du projet de loi;

c) Principe de finalité : article 2 du projet de loi;

d) Principe de l'accès par les personnes concernées : articles 11 et 12 du projet de loi;

e) Principe de non-discrimination : article 20 du projet de loi;

f) Faculté de dérogation : article 13 du projet de loi;

g) Principe de sécurité : article 8 du projet de loi;

h) Contrôle et sanctions : articles 21 à 25 et 27 du projet de loi;

i) Flux transfrontières de données : article 26 du projet de loi.

III. INFORMATIONS EMANANT D'ORGANISATIONS INTERGOUVERNEMENTALES

A. Conseil de l'Europe

[Original : anglais]
[12 août 1994]

79. La Commission européenne des droits de l'homme du Conseil de l'Europe a indiqué qu'en vertu de l'article 8 de la Convention européenne des droits de l'homme, elle avait été appelée à connaître d'affaires relatives à l'utilisation des fichiers contenant des données à caractère personnel par les autorités nationales. Toutefois, les décisions concernant les fichiers de données informatisés étaient très peu nombreuses. La Commission a joint le texte de sa décision n° 10473/83 du 11 décembre 1985 (Tom Lundvall c. Suède)*.

B. Interpol

[Original : français]
[9 août 1994]

80. L'organisation internationale de police criminelle (Interpol) a communiqué les informations suivantes :

RESPECT PAR L'O.I.P.C.-INTERPOL DES PRINCIPES DIRECTEURS APPLICABLES AUX FICHIERS INFORMATISES CONTENANT DES DONNEES A CARACTERE PERSONNEL

Introduction

Le principe de la protection des données détenues par le Secrétariat général de l'O.I.P.C.-Interpol fait l'objet d'un traité (l'Accord de Siège et l'Echange de lettres de 1982) entre le Gouvernement de la République française et l'Organisation, ainsi que d'une réglementation interne "Règlement relatif à la coopération policière internationale et au contrôle interne des fichiers de l'O.I.P.C.-Interpol". Les textes de ces trois instruments juridiques, ainsi que le Statut de l'Organisation* constituent le cadre légal régissant l'application des principes directeurs énoncés dans le document E/CN.4/1990/72, tels qu'ils ont été intégrés dans l'ordre juridique de l'Organisation.

1. Dérogation à la loi nationale du pays de Siège

L'Accord de Siège de 1982, entré en vigueur le 14 février 1984, déclare inviolables le siège, les archives et la correspondance de l'Organisation (articles 4, 7 et 9). Il dispose également que les "fichiers (d'Interpol) sont soumis au contrôle interne mis en oeuvre par l'Organisation selon les règles générales fixées par échange de lettres avec le Gouvernement de la République française"(article 8).

---

* Les textes peuvent être consultés au Secrétariat.

Cet échange de lettres soumet les fichiers détenus par le Secrétariat général de l'O.I.P.C.-Interpol au contrôle d'une Commission indépendante dont la création incombe à l'Organisation. Sa composition, son fonctionnement et le principe de contrôles auxquels elle doit procéder sont définis avec force et clarté dans les dispositions dudit Echange de lettres.

Il en résulte que les fichiers de l'O.I.P.C.-Interpol sont couverts par les dispositions de l'Accord de Siège et exemptés du contrôle de la Commission Nationale de l'Informatique et des Libertés (C.N.I.L.), organe français chargé de veiller au respect de la loi de 1978 sur la protection des données en France.

2. Désignation de l'autorité statutairement compétente pour contrôler la bonne application des principes directeurs

L'Organisation a honoré son engagement énoncé dans l'Echange de lettres par l'adoption du "Règlement relatif à la coopération policière internationale et au contrôle interne des fichiers de l'O.I.P.C.-Interpol". Ce règlement, appelé ci-après "Règlement coopération", est l'acte par lequel l'Organisation a créé la Commission de contrôle interne des fichiers de l'O.I.P.C.-Interpol.

Cette institution de contrôle est un organe subsidiaire de l'Organisation qui l'a désigné comme étant "l'autorité statutairement compétente pour contrôler l'application" des règles adoptées par l'O.I.P.C.-Interpol en matière de protection de données nominatives.

La création de cette Commission dont la composition et le fonctionnement sont décrits aux articles 15 et suivants du "Règlement coopération", correspond donc aux recommandations énoncées dans le point (B) du document E/CN.4/1990/72 en ce qui concerne les organisations internationales.

Il importe de signaler que M. Louis JOINET, magistrat/conseiller technique au Cabinet du Premier Ministre Français à l'époque de la négociation de l'Accord de siège entre l'O.I.P.C.-Interpol et la France et rapporteur de la Commission des droits de l'homme de l'ONU, a évoqué cet organe comme une institution susceptible de servir de modèle pour le contrôle des fichiers de nombreuses organisations internationales ayant leur siège en France.

3. Contenu des principes directeurs adoptés par l'O.I.P.C.-Interpol

L'O.I.P.C.-Interpol a intégré "les principes directeurs applicables aux fichiers contenant des données à caractère personnel, détenus par les organisations internationales gouvernementales" dans son ordre juridique interne de la manière suivante :

Principe de licéité et de loyauté (n° 1)

Ce principe est consacré par le Statut de l'O.I.P.C.-INTERPOL, notamment l'article 2 qui énonce les missions principales de l'Organisation, délimite sa compétence et fait une référence expresse tant à l'esprit de la Déclaration universelle des droits de l'homme qu'au respect des lois existant dans les différents Etats traitant avec Interpol par l'intermédiaire des Bureaux Centraux Nationaux qui font partie de leurs autorités nationales.

Comme conséquence de ce principe, l'article 1er alinéa 2 du "Règlement coopération" précise que son but est "de protéger contre tout abus les informations de police traitées et communiquées au sein du système de la coopération policière internationale mis en place par l'O.I.P.C.-Interpol, notamment en vue de prévenir toute atteinte aux droits des individus".

Le respect du principe de licéité implique, à son tour, le respect de deux règles juridiques fondamentales dans le Système d'Interpol. Il s'agit des articles 5(3) et 3(3) du "Règlement coopération".

L'article 5(3) dudit Règlement dispose "que le Secrétariat général n'est que dépositaire des informations de police qui lui sont communiquées" par les autorités de police nationales. Il ressort de cette disposition que les autorités de police nationales (qui sont la source principale des informations pour Interpol) sont tenues de vérifier la légitimité et la légalité de la communication des informations qu'elles désirent divulguer à l'Organisation.

Une fois l'information communiquée au Secrétariat général, son traitement, son enregistrement et sa communication sont soumis à des règles propres à l'Organisation. C'est ainsi que l'article 3 (3) du "Règlement coopération" dispose que "le traitement d'informations de police par le Secrétariat général ... n'est assujetti à aucune législation nationale. Il est effectué conformément aux dispositions du présent Règlement et des accords conclus avec l'Etat du siège".

Principe d'exactitude (n° 2)

Plusieurs dispositions du "Règlement coopération" consacrent ce principe comme une obligation à la charge tant du Secrétariat général de l'Organisation que du pays à l'origine de l'information déposée au Secrétariat général. Il en est ainsi des articles 5(2), 6(2), 6(3), 7(5) et 9(4) du "Règlement coopération".

L'obligation de détenir des informations exactes engendre non seulement une obligation de mise à jour, mais également une obligation d'épuration de ces informations. C'est ainsi que l'article 5(5) du "Règlement coopération" dispose que "La destruction, par le Secrétariat général, d'informations de police considérées comme périmées en fonction de certains critères généraux sera déterminée par un règlement particulier approuvé par l'Assemblée générale". Ce Règlement a été adopté en 1987.

Principe de finalité (n° 3)

Conformément à l'article 3(4) du "Règlement coopération", "le traitement d'informations de police par le Secrétariat général s'exerce dans un but de prévention et de répression des infractions pénales de droit commun au sens de l'article 2, paragraphe (b) du Statut et ne tombant pas sous le coup de l'article 3 du Statut, dans l'intérêt des investigations les concernant, pour la recherche de personnes disparues, ainsi que pour l'identification de cadavres".

Ce principe est également consacré par l'article 22(b) du "Règlement coopération", qui charge la Commission de contrôle interne des fichiers de s'assurer que les informations détenues par le Secrétariat général sont enregistrées et traitées pour des finalités déterminées.

Les données à caractère personnel collectées et traitées par le Secrétariat général servent donc à des fins de police. C'est la raison pour laquelle l'Organisation a dérogé au principe de publicité ou d'information de la personne concernée avant l'utilisation ou la divulgation des données aux autorités de police intéressées, conformément au principe n° 6 prévoyant la faculté de dérogation.

Principe de l'accès par les personnes concernées (n° 4)

Ce principe est consacré par l'article 23 du "Règlement coopération" qui prévoit la possibilité pour les personnes éventuellement intéressées de demander à la Commission de contrôle la vérification des informations les concernant. La Commission notifiera ensuite au demandeur que ces vérifications ont été effectuées, sans révéler le contenu des informations détenues. Il s'agit donc d'un droit d'accès indirect des individus aux fichiers de police de l'Organisation.

Cet accès indirect aux fichiers de police se justifie par la différence de finalité entre un fichier national et un fichier international de police géré par l'Organisation dépositaire des informations qui lui sont confiées. En effet, il n'appartient pas à l'Organisation d'apprécier si la divulgation d'une information de police peut nuire à l'ordre public d'un Etat membre ou porter atteinte à la coopération entre deux ou plusieurs Etats membres.

Grâce à ce système mis en place par l'Organisation, de nombreuses personnes qui ne peuvent bénéficier d'un droit d'accès, même indirect, aux fichiers de police de leur pays peuvent l'exercer sur un plan international.

Principe de non-discrimination (n° 5)

Sous réserve des besoins d'identification de la personne recherchée sur le plan international et de description des faits constitutifs d'infractions pénales de droit commun, ce principe est consacré par l'article 3 du Statut de l'Organisation qui lui interdit d'intervenir dans les affaires à caractère politique, militaire, religieux ou racial.

Faculté de dérogation (n° 6)

Les normes adoptées par l'Organisation en matière de protection des données correspondent aux principes énoncés par le document E/CN.4/1990/72 des Nations Unies, sous réserve des dérogations ou adaptations justifiées par la nature spécifique des activités de l'O.I.P.C.-Interpol, ces adaptations étant autorisées par le point (B) et le principe n° 6 du point (A) du document E/CN.4/1990/72 prévoyant "la faculté de dérogation" à certains principes pour protéger la sécurité, l'ordre public et les droits et libertés d'autrui.

En outre, l'Organisation s'acquitte d'une mission humanitaire dans le cadre des recherches de personnes disparues et de l'identification de cadavres. Les fonctions de l'Organisation dans ce domaine ne sont que la prolongation internationale de la mission humanitaire de la police sur le plan national.

Enfin, conformément à l'article 3, alinéas 3 et 4 du "Règlement coopération", toutes les données de police peuvent également être utilisées pour la gestion interne ainsi que pour la recherche et la publication scientifiques

et la poursuite de tout autre but légitime, à condition que l'identification des personnes éventuellement concernées soit rendue impossible.

Principe de sécurité (n° 7)

L'article 1er, alinéa 2, (cité ci-dessus) du "Règlement coopération", qui prohibe tout abus d'utilisation d'informations de police, et l'article 4 dudit Règlement, consacrent ce principe de sécurité. C'est ainsi que l'article 4 du "Règlement coopération" dispose que "le Secrétariat général prend les précautions nécessaires afin de préserver le secret et la sécurité des informations de police et d'empêcher que ces informations ne soient traitées ou communiquées d'une façon illicite ou abusive". Cet article dispose également que "les personnels du Secrétariat général sont tenus au secret professionnel". Cette obligation de secret professionnel est mise également à la charge des membres de la Commission de contrôle conformément à l'article 19 dudit Règlement.

Des mesures de protection informatiques sophistiquées et des procédures administratives rigoureuses ont également été mises au point par le Secrétariat général pour protéger les données contre toute altération ou accès non autorisé.

Contrôle et sanctions (n° 8)

Conformément à l'article 22 du "Règlement coopération", la Commission de contrôle interne des fichiers de l'O.I.P.C.-Interpol a pour attribution principale de s'assurer que les informations à caractère personnel contenues dans les fichiers d'Interpol sont obtenues, traitées et conservées conformément aux principes énoncés dans le présent document.

Pour mener à bien ses attributions de contrôle général, la Commission dispose d'un accès direct à tous les fichiers de l'organisation et d'un droit d'investigation qu'elle peut invoquer à l'égard du Secrétariat général. Elle peut également consulter le Comité exécutif de l'Organisation ainsi que les autorités de police d'un pays à l'origine de l'information soumise à sa vérification. En vue d'exercer cette mission de contrôle général, la Commission procède à des vérification soit à la demande d'un particulier soit d'office en examinant des dossiers de police qu'elle sélectionne de manière aléatoire.

La Commission peut demander la modification ou la destruction de l'information détenue par le Secrétariat général conformément à l'article 24 (3) du "Règlement coopération". Le résultat de son contrôle et de ses investigations est notifié au Comité exécutif de l'Organisation afin que les organes compétents procèdent aux modifications nécessaires conformément à l'article 25 du "Règlement coopération".

Flux transfrontières de données (n° 9)

La circulaire des informations entre le Secrétariat général et les autorités de police des Etats membres ou les autres entités habilitées est régie tant par les principes énoncés ci-dessus que par plusieurs dispositions spécifiques du "Règlement coopération" (articles 5, 7, 8 et 9) qui subordonnent la communication des informations de police aux autorités de police ou aux autres entités nationales ou internationales à des conditions strictes.

Champs d'application (n° 10)

Deux sortes de fichiers nominatifs sont détenus par le Secrétariat général de l'Organisation : les fichiers de police et les fichiers administratifs.

Les principes exposés ci-dessus s'appliquent aux fichiers de police manuels ou automatisés (Criminal Information System).

Quant aux fichiers administratifs, ils comportent les fichiers du personnel de l'Organisation et des personnes qui ont un contact officiel avec elle. Ces fichiers ne sont pas soumis aux mêmes règles juridiques que celles régissant les fichiers de police. Cela n'empêche par l'Organisation de respecter les principes directeurs énoncés dans le document E/CN.4/1990/72, sous réserve de leur adaptation aux nécessités de bon fonctionnement de l'Organisation et de la vérification de la Commission de contrôle interne des fichiers de l'O.I.P.C.-Interpol.

En résumé, les informations détenues par le Secrétariat général sur son personnel et ses cocontractants ou visiteurs sont collectées d'une manière licite à partir des déclarations des intéressés eux-mêmes et des sources publiques (registres civils ou commerciaux, autorités nationales, organes internationaux etc.) et tenant compte de la mise à jour effectuée par les intéressés ou les services compétents du Secrétariat général, après vérification de leur exactitude. Ces fichiers administratifs ont une finalité de gestion, de comptabilité, de protection sociale, d'administration et toute autre finalité conforme aux buts et objectifs de l'Organisation tels qu'ils sont énoncés dans son Statut et ses Règlements internes.

Aussi, le Statut et le Règlement du personnel intègrent-ils les principes de la fonction internationale publique adaptant certains principes énoncés dans le document E/CN.4/1990/72. Ils autorisent le personnel à avoir un accès direct à son fichier. Les données concernant le personnel sont confidentielles et ne sont utilisées que pour leur finalité de gestion et d'administration. Tout accès non autorisé ou non justifié par des nécessités de service est prohibé. La violation de ces principes peut donner lieu à des procédures disciplinaires, soumises au contrôle du Tribunal Administratif de l'O.I.T.

Annexe

PRINCIPES DIRECTEURS APPLICABLES AUX FICHIERS INFORMATISES CONTENANT DES DONNEES A CARACTERE PERSONNEL

Les modalités d'application des règlements concernant les fichiers informatisés contenant des données à caractère personnel sont laissées à la libre initiative de chaque Etat sous réserve des orientations suivantes :

A. Principes concernant les garanties minimales qui devraient être prévues dans les législations nationales

1. PRINCIPE DE LICEITE ET DE LOYAUTE

Les données concernant les personnes ne devraient pas être obtenues ou traitées à l'aide de procédés illicites ou déloyaux, ni utilisées à des fins contraires aux buts et aux principes de la Charte des Nations Unies.

2. PRINCIPE D'EXACTITUDE

Les personnes responsables de l'établissement d'un fichier ou celles responsables de leur mise en oeuvre devraient être tenues de vérifier l'exactitude et la pertinence des données enregistrées et de veiller à ce qu'elles demeurent aussi complètes que possible pour éviter les erreurs par omission et qu'elles soient mises à jour, périodiquement ou lors de l'utilisation des informations contenues dans un dossier, tant qu'elles font l'objet d'un traitement.

3. PRINCIPE DE FINALITE

La finalité en vue de laquelle est créé un fichier et son utilisation en fonction de cette finalité devraient être spécifiées, justifiées et, lors de sa mise en oeuvre, faire l'objet d'une mesure de publicité ou être portées à la connaissance de la personne concernée, afin qu'il soit ultérieurement possible de vérifier :

a) Si toutes les données personnelles collectées et enregistrées restent pertinentes par rapport à la finalité poursuivie;

b) Si aucune desdites données personnelles n'est utilisée ou divulguée, sauf accord de la personne concernée, à des fins incompatibles avec celles ainsi spécifiées;

c) Si la durée de conservation des données personnelles n'excède pas celle permettant d'atteindre la finalité pour laquelle elles ont été enregistrées.

4. PRINCIPE DE L'ACCES PAR LES PERSONNES CONCERNEES

Toute personne justifiant de son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs, d'obtenir les rectifications ou destructions adéquates en cas d'enregistrements illicites, injustifiés ou inexacts, et, lorsqu'elles sont communiquées, d'en connaître les

destinataires. Une voie de recours devrait être prévue, le cas échéant, auprès de l'autorité de contrôle prévue au principe 8 ci-dessous. En cas de rectification, le coût devrait être à la charge du responsable du fichier. Il est souhaitable que les dispositions de ce principe s'appliquent à toute personne, quelle que soit sa nationalité ou sa résidence.

5. PRINCIPE DE NON-DISCRIMINATION

Sous réserve des cas de dérogations limitativement prévus sous le principe 6, les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées.

6. FACULTE DE DEROGATION

Des dérogations aux principes 1 à 4 ne peuvent être autorisées que si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques ainsi que, notamment, les droits et libertés d'autrui, spécialement de personnes persécutées (clause humanitaire), sous réserve que ces dérogations soient expressément prévues par la loi ou par une réglementation équivalente prise en conformité avec le système juridique interne qui en fixe expressément les limites et édicte des garanties appropriées.

Les dérogations au principe 5 relatif à la prohibition de la discrimination, outre qu'elles devraient être soumises aux mêmes garanties que celles prévues pour les dérogations aux principes 1 à 4, ne pourraient être autorisées que dans les limites prévues par la Charte internationale des droits de l'homme et les autres instruments pertinents dans le domaine de la protection des droits de l'homme et de la lutte contre les discriminations.

7. PRINCIPE DE SECURITE

Des mesures appropriées devraient être prises pour protéger les fichiers tant contre les risques naturels, tels que la perte accidentelle ou la destruction par sinistre, que les risques humains, tels que l'accès non autorisé, l'utilisation détournée de données ou la contamination par des virus informatiques.

8. CONTROLE ET SANCTIONS

Chaque législation devrait désigner l'autorité qui, en conformité avec le système juridique interne, est chargée de contrôler le respect des principes précités. Cette autorité devrait présenter des garanties d'impartialité, d'indépendance à l'égard des personnes ou organismes responsables des traitements et de leur mise en oeuvre, et de compétence technique. En cas de violation des dispositions de la loi interne mettant en oeuvre les principes précités, des sanctions pénales ou autres devraient être prévues ainsi que des recours individuels appropriés.

9. FLUX TRANSFRONTIERES DE DONNEES

Lorsque la législation de deux ou plusieurs pays, concernés par un flux transfrontières de données, présente des garanties comparables au regard de la protection de la vie privée, les informations doivent pouvoir circuler aussi librement qu'à l'intérieur de chacun des territoires concernés. En l'absence de garanties comparables, des limitations à cette circulation ne peuvent être imposées indûment et seulement dans la stricte mesure où la protection de la vie privée l'exige.

10. CHAMP D'APPLICATION

Les présents principes devraient s'appliquer en premier lieu à tous les fichiers informatisés publics et privés et, par voie d'extension facultative et sous réserve des adaptations adéquates, aux fichiers traités manuellement. Des dispositions particulières également facultatives pourraient être prises pour étendre tout ou partie desdits principes aux fichiers de personnes morales, notamment lorsqu'ils contiennent pour partie des informations concernant des personnes physiques.

B. Application des principes directeurs aux fichiers contenant des données à caractère personnel, détenus par les organisations internationales gouvernementales

Les présents principes directeurs devraient être applicables aux fichiers contenant des données à caractère personnel détenus par les organisations internationales gouvernementales sous réserve des adaptations nécessaires pour tenir compte des différences qui peuvent exister entre les fichiers à finalités internes tels que ceux qui concernent la gestion du personnel et les fichiers à finalités externes concernant les tiers en relation avec l'organisation.

Chaque organisation devrait désigner l'autorité statutairement compétente pour contrôler la bonne application des présents principes directeurs.

Clause humanitaire : une dérogation à ces principes devrait être spécifiquement prévue lorsque le fichier a pour finalité la protection des droits de l'homme et des libertés fondamentales de la personne concernée ou l'assistance humanitaire.

Une dérogation de même portée devrait être prévue dans la loi nationale en faveur des organisations internationales gouvernementales dont l'accord de siège n'aurait pas écarté l'application de ladite législation nationale, ainsi qu'en faveur des organisations internationales non gouvernementales auxquelles ladite loi serait applicable.