NATIONS UNIES **E**

Conseil Economique et Social

Distr.
GENERALE

E/CN.4/1997/67
23 janvier 1997

FRANCAIS
Original : ANGLAIS/ARABE/
ESPAGNOL/FRANCAIS

COMMISSION DES DROITS DE L'HOMME
Cinquante-troisième session
Point 12 de l'ordre du jour provisoire

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 1995/114 de la Commission

TABLE DES MATIERES

Introduction

1. Dans sa décision 1995/114 du 8 mars 1995, 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, et prenant note du rapport du Secrétaire général présenté en application de sa décision 1993/113 (E/CN.4/1995/75), a décidé :

a) De demander aux Etats, aux organisations intergouvernementales, régionales et non gouvernementales de coopérer pleinement avec le Secrétaire général pour lui fournir toutes les informations pertinentes relatives à l'application des principes directeurs;

b) De prier le Secrétaire général de continuer à veiller à la mise en oeuvre des principes directeurs au sein du système des Nations Unies;

c) De demander au Secrétaire général de lui faire rapport à sa cinquante-troisième session :

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

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

2. En application de cette décision, le Secrétaire général a, le 6 juin 1996, demandé aux organes, organismes, commissions régionales et institutions spécialisées des Nations Unies ainsi qu'aux organisations apparentées de lui communiquer des informations sur l'application des principes directeurs dans les services 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. Au 10 décembre 1996, le Secrétariat avait reçu des réponses des organes, organismes et institutions spécialisées des Nations Unies indiqués ci-après : Division de la prévention du crime et de la justice pénale, Département des affaires humanitaires, Commission économique pour l'Europe, Commission économique pour l'Amérique latine et les Caraïbes, Programme des Nations Unies pour l'environnement, Fonds des Nations Unies pour la population, Programme alimentaire mondial, Agence internationale de l'énergie atomique, Organisation internationale du Travail, Fonds monétaire international, Union internationale des télécommunications, Organisation des Nations Unies pour l'éducation, la science et la culture.

5. Des informations ont été communiquées par les gouvernements des pays suivants : Allemagne, Argentine, Autriche, Croatie, Estonie, Jamahiriya arabe libyenne, Luxembourg, Maurice, Mexique, Philippines, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Saint-Marin, Suède et Uruguay.

6. Une réponse a été reçue d'une organisation intergouvernementale : l'Organisation des Etats américains qui a dit n'être pas en mesure de donner les renseignements demandés.

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 33 organes, organismes, commissions régionales et institutions spécialisées des Nations Unies et organisations apparentées auxquels des demandes avaient été adressées, 12 seulement ont répondu.

10. Le Département des affaires humanitaires, la Commission économique pour l'Amérique latine et les Caraïbes et l'Union internationale des télécommunications ont indiqué qu'ils n'avaient aucune information à communiquer ou observation à formuler sur le sujet.

11. La Commission économique pour l'Europe (CEE) a fait savoir que les décisions de la Commission des droits de l'homme ne s'appliquaient à aucune de ses activités car ses fichiers statistiques étaient soit anonymes soit agrégés.

12. Le Programme des Nations Unies pour l'environnement a indiqué que sa pratique était conforme aux dispositions des principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel.

13. L'Agence internationale de l'énergie atomique a indiqué que les dispositions de la section 8 de son manuel administratif, qui traite de la protection des renseignements confidentiels concernant le personnel étaient conformes aux principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptés par l'Assemblée générale.

14. Le Fonds monétaire international (FMI) a aussi fait savoir que les procédures en vigueur au FMI pour la gestion des fichiers personnels et l'accès à ces fichiers semblaient concorder étroitement avec les principes directeurs.

15. L'Organisation des Nations Unies pour l'éducation, la science et la culture a confirmé qu'elle souscrivait aux principes directeurs pour la réglementation des fichiers contenant des données à caractère personnel.

16. Le Fonds des Nations Unies pour la population a indiqué que toutes les questions concernant le personnel étaient gérées par le PNUD et qu'il suivait donc les directives de l'ONU/PNUD, lesquelles correspondaient aux principes énoncés dans le document E/CN.4/1990/72 et dans la résolution 45/95 de l'Assemblée générale.

17. Le Programme alimentaire mondial (PAM) a fait parvenir la déclaration suivante :

> "Les données informatisées à caractère personnel relatives aux fonctionnaires directement employés par le PAM sont conservées par l'Organisation des Nations Unies pour l'alimentation et l'agriculture (FAO) dont le siège est à Rome, avec laquelle nous partageons un système informatisé de données à caractère personnel (Persys). La FAO assume la responsabilité et la gestion de ce système. Les fonctionnaires

du service des ressources humaines du PAM ont un accès restreint aux fichiers informatisés concernant le personnel du PAM uniquement.

A notre connaissance, le système Persys de la FAO satisfait à tous les principes énoncés dans le document E/CN.4/1990/72, en date du 20 février 1990."

18. La Division de la prévention du crime et de la justice pénale (Office des Nations Unies à Vienne) a communiqué les informations suivantes :

"1. Dans ses activités, la Division se réfère souvent aux 'principes directeurs'. En particulier, elle les a incorporés dans les publications suivantes destinées à la vente :

a) 'Guide pour l'informatisation des systèmes d'information en justice pénale' (ST/ESA/STAT/SER.F/58, Publication des Nations Unies, numéro de vente : F.92.XVII.6, p. 174), établi conjointement par la Division de statistique du Siège et notre division;

b) 'Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique' (Revue internationale de politique criminelle, No 43/44 de 1994, ST/ESA/SER.M/43 et 44, Publication des Nations Unies, numéro de vente : F.94.IV.5, par. 138).

2. Il est également fait mention des principes directeurs dans les documents de travail établis par la Division pour les huitième et neuvième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, tenus en 1990 et en 1995 respectivement, en particulier dans les documents suivants :

a) A/CONF.144/14, Informatisation de l'administration de la justice pénale, par. 12;

b) A/CONF.169/6, Systèmes de justice pénale et de police : gestion et amélioration de la police et d'autres services de répression, du parquet, des tribunaux et du système pénitentiaire, et rôle des avocats, par. 89.

3. Dans le cadre des activités de formation des membres des professions liées à l'exercice de la justice pénale, qui sont surtout mises en place dans les pays en développement, des experts invités par la Division et les fonctionnaires de celle-ci informent les intéressés de la nécessité de protéger la vie privée dans la gestion des dossiers personnels informatisés ou de recherche manuelle des auteurs présumés d'infractions et des condamnés, conformément aux dispositions des 'Principes directeurs'. Tout récemment, la Division a traité des questions liées à la protection de la vie privée lors d'un séminaire de formation interrégional sur le Réseau d'information des Nations Unies sur la criminalité et la justice et l'échange de données avec les pays en développement, qui était organisé par le Gouvernement de la République de Corée, sous les auspices de l'Organisation des Nations Unies (Séoul, 9-13 septembre 1996).

4. Enfin il est apparu, au cours de diverses consultations officieuses avec des spécialistes de la criminalité informatique et dans le contexte des activités de la Division, que les principes directeurs pourraient être utiles pour l'administration de la justice pénale dans les pays si leurs dispositions pouvaient couvrir deux tendances générales qui se dégagent actuellement :

a) La menace croissante que représentent la criminalité organisée et le terrorisme;

b) L'évolution très rapide des nouvelles technologies dans le domaine du traitement de l'information.

5. Ces deux tendances ont des incidences sur le fonctionnement des systèmes de justice pénale et sur le rôle des organes chargés de l'application des lois (les principes 1 à 4 soulignent que les données doivent être obtenues à l'aide de procédés licites et loyaux), ce qui peut compromettre la protection de la vie privée (le principe 6 porte sur la 'faculté de dérogation').

6. Pour favoriser l'obtention de données par des moyens licites et loyaux et assurer l'application des principes directeurs dans l'ensemble des pays, il pourrait être utile d'envisager de faire le bilan de la situation sur au moins deux points :

a) Depuis 1990 (année de l'adoption des principes directeurs), les pays ont-ils adopté des lois sur la protection des données ?

b) Le public est-il tenu informé de l'établissement et du mode de gestion des bases de données informatiques en matière de justice pénale qui sont établies et gérées (systèmes perfectionnés de reconnaissance visuelle/télévision en circuit fermé, reconnaissance informatisée des visages, bases de données nationales sur l'ADN contenant les empreintes génétiques des auteurs présumés d'infractions, systèmes intelligents d'observation des routes et de la circulation, cartes d'identité et autres cartes à mémoire facilitant diverses transactions personnelles)."

19. L'Organisation internationale du Travail (OIT) a communiqué les informations suivantes :

"En ce qui concerne l'application des principes directeurs au Bureau international du Travail (BIT), le BIT n'a pas encore créé de fichiers personnels informatisés à proprement parler. Ces fichiers, toujours sur papier, sont gérés manuellement. Cependant, le Bureau est en train de mettre en place un Système d'information sur le personnel (PERSIS) qui comprend plusieurs bases de données informatisées. PERSIS est basé sur le Système intégré de gestion (SIG) mis au point par le Secrétariat de l'Organisation des Nations Unies à New York, et l'on peut penser que celui-ci est conforme aux principes directeurs.

Les différents principes directeurs sont, dans la pratique, pleinement respectés par le BIT :

- Principe de licéité et de loyauté : respecté;

- Principe d'exactitude : apurement et actualisation permanents des fichiers;

- Principe de finalité : toutes les données du Système intégré de gestion (SIG) sont directement utiles pour la gestion du personnel et des états de paye, et il n'y a pas dans le système de renseignements non pertinents;

- Principe de l'accès par les personnes concernées : respecté;

- Principe de non-discrimination : respecté;

- Faculté de dérogation : respecté;

- Principe de sécurité : le serveur de la base de données est très protégé au sein du réseau du BIT et le BIT vient d'installer un logiciel de filtrage très strict pour protéger ses fichiers contre l'accès non autorisé;

- Contrôle et sanctions : respecté;

- Flux transfrontières de données : respecté;

- Champ d'application : respecté."

20. L'OIT a en outre fait mention de la Réunion d'experts sur la protection de la vie privée des travailleurs, qui devait se tenir à Genève du 1er au 7 octobre 1996. Cette réunion devait examiner un projet de recueil de directives pratiques sur la protection des données personnelles des travailleurs ainsi que d'éventuelles autres actions de la part de l'OIT. Ce projet porte sur tout usage des données personnelles, y compris leur collecte, leur stockage et leur communication.

II. INFORMATIONS COMMUNIQUEES PAR DES ETATS

Allemagne

[Original : anglais]
[12 septembre 1996]

1. Pour se conformer à la directive 95/46 du 24 octobre 1995 du Parlement européen et du Conseil sur la protection des données, les Etats membres de l'UE doivent en général adapter leur législation nationale. Les dispositions de la directive doivent être adoptées le 23 octobre 1998 au plus tard. La plupart des prescriptions de la directive sont cependant déjà incorporées dans la loi allemande sur la protection des données. A l'heure actuelle, et par rapport à ce qui est indiqué dans le document E/CN.4/1990/72, la situation concernant certains des principes directeurs des Nations Unies progresse comme suit :

Principe 4

2. La protection des données sera rendue plus transparente pour le citoyen. A cette fin, les moyens suivants seront notamment utilisés : l'obligation d'informer la personne fichée du stockage ou de la communication des données la concernant sera étendue au secteur public; l'obligation générale d'informer la personne fichée de la collecte de données la concernant sera appliquée aussi au secteur privé; le droit d'accès de la personne fichée sera légèrement élargi.

Principe 9

3. Pour adapter la législation sur la protection des données à la directive de la CE, il faudra y introduire une disposition assujettissant la communication des données à un pays tiers à l'existence d'une protection suffisante des données dans ce pays. De plus, l'adoption d'une liste complète de dérogations à ce principe s'impose afin de ne pas compromettre les échanges avec les pays tiers. Il convient par ailleurs de prévoir une réglementation pour empêcher le transfert des processeurs de données dans des Etats non membres de l'UE où la protection des données est moindre en rendant applicables aussi dans ces Etats les dispositions nationales qui transposent la directive de la CE, si les moyens de traitement, tels que terminaux, questionnaires, etc., se trouvent sur le territoire d'un Etat membre de la CE.

Argentine

[Original : espagnol]
[22 août 1996]

1. Depuis la réforme constitutionnelle d'août 1994, la Constitution argentine prévoit, au paragraphe 3 de son article 43, le recours en amparo que toute personne peut former 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, d'en connaître la finalité et, en cas d'erreur ou de discrimination, d'exiger la suppression, la rectification, le classement comme confidentielles ou la mise à jour.

2. Cette disposition constitutionnelle reflète les principes directeurs adoptés par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990 et la décision 1995/114 de la Commission des droits de l'homme, en date du 8 mars 1995. Parmi les principes sur lesquels repose cette disposition, il y a lieu de citer tout particulièrement le principe de finalité (par. 3); le principe de l'accès par les personnes concernées (par. 4); le principe de non-discrimination (par. 5); le principe relatif au contrôle et aux sanctions (par. 8); et le principe concernant le champ d'application aux fichiers publics et privés (par. 10).

3. Dans le domaine législatif, le Congrès national a été saisi de 18 projets de loi, dont un seul à ce jour a été approuvé par la Chambre des députés du Congrès à sa séance du 5 juin 1996.

4. Ce projet reprend entièrement les principes directeurs et autorise des dérogations selon les prescriptions énoncées au paragraphe 6. Par ailleurs, il donne une définition claire des concepts utilisés afin d'éviter toute ambiguïté conceptuelle qui pourrait nuire à son application et à son efficacité.

5. En ce qui concerne l'autorité chargée d'assurer l'application des dispositions pertinentes, l'article 5 du projet institue, dans le cadre du Congrès national, une commission bicamérale pour le contrôle de la protection des données (Comisión Bicameral de Seguimiento de Protección de Datos) qui est chargée de veiller à la protection des droits visés par la loi.

6. Il y a lieu de commenter l'article 11 du projet, qui prévoit que certaines données à caractère personnel doivent être particulièrement protégées; il s'agit des données concernant i) l'idéologie, la race, la religion, les habitudes personnelles et le comportement sexuel; ii) l'état de santé (à cet égard, l'article 12 établit une dérogation autorisant la communication aux établissements médicaux et spécialisés des informations pertinentes sur les personnes qui viennent consulter ou recevoir un traitement), la situation patrimoniale et les obligations fiscales, une dérogation n'étant possible que pour des motifs liés à l'intérêt général et si elle est prévue par la loi ou avec le consentement de l'intéressé; iii) les données concernant les poursuites pénales ou les infractions administratives, lesquelles ne peuvent figurer que dans les fichiers ou bases de données des administrations publiques compétentes, conformément à leur réglementation respective.

7. Le projet dispose également que les données à caractère personnel ne peuvent être cédées qu'avec le consentement préalable de l'intéressé, donné par écrit - et à tout moment révocable - et que la cession est frappée de nullité si sa finalité n'apparaît pas clairement (art. 15). Le consentement de l'intéressé n'est pas exigé dans les cas spécifiquement prévus par le projet et qui touchent à des considérations d'intérêt public comme la bonne administration de la justice et la santé publique.

8. La transmission de données de caractère personnel à l'extérieur du pays, qu'il s'agisse des organismes internationaux ou supranationaux, doit bénéficier de la même protection qu'au sein de la République.

9. Toute personne sur laquelle portent les informations contenues dans les fichiers a le droit : i) de contester les actes administratifs ou les décisions de caractère privé qui sont uniquement fondés sur l'évaluation qui peut être faite de l'intéressé à partir du traitement de données à caractère personnel; ii) d'être informée de l'existence des fichiers ou bases de données, de leur finalité et de l'identité de la personne ou de l'autorité responsable; iii) de demander et d'obtenir communication des informations à caractère personnel inscrites dans les fichiers ou bases de données sans qu'aucune contrepartie soit exigée; iv) de faire rectifier, supprimer ou conserver les données à caractère personnel.

10. S'agissant de la protection des droits, le projet prévoit la possibilité d'intenter une action en justice pour établir les responsabilités en ce qui concerne les dommages aux biens ou les atteintes aux droits subis par l'intéressé du fait des informations collectées, action qui devra conduire à réparation sous la forme d'une indemnisation. Cette action, qui suit la voie de la procédure sommaire n'empêche pas la formation du recours en amparo prévu par la Constitution et conformément à la loi 16.986, lequel, en vertu de l'article 321 du Code civil et de procédure, suit une procédure simplifiée.

11. S'agissant des personnes responsables des fichiers ou banques de données - et sans préjudice des responsabilités liées aux dommages et aux préjudices occasionnés à l'intéressé ni des sanctions pénales dont seraient passibles les infractions commises - le projet prévoit l'application de sanctions telles qu'avertissement, suspension, amende, suppression ou fermeture des fichiers ou banques de données par le Défenseur du peuple qui, d'après la réglementation que devrait adopter la Commission bicamérale créée par la loi, sera l'autorité responsable de l'application des dispositions de celle-ci.

12. Au dernier article du projet les provinces sont invitées à créer des fichiers ou banques de données provinciaux et à désigner les autorités responsables en la matière; en tout état de cause, le projet dispose que le défaut de réglementation procédurale n'empêchera pas la formation du recours selon la procédure rapide prévue à l'article 43 de la Constitution nationale.

13. Les informations présentées dans les paragraphes ci-dessus sont un résumé des mesures récentes que la République argentine a prises dans le domaine considéré. A toutes fins utiles, ont trouvera ci-joint copie du texte intégral du projet de loi présenté *.

Autriche

[Original : anglais]
[11 septembre 1996]

1. La Loi sur la protection des données (Datenschutzgesetz - DSG), publiée dans le Journal officiel fédéral No 565/1978 reprend tous les éléments des Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel. En particulier,

---

*Le texte peut être consulté au secrétariat.

les concepts de finalité (principe 3), ainsi que de licéité et de loyauté (principe 1) et la faculté de dérogation limitée à certains cas (principe 6) sont les fondements de la protection des données en Autriche, comme il ressort de la section 1 de la loi.

2. Le principe 5 est couvert par l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe que l'Autriche a ratifiée en 1988 (Journal officiel fédéral No 317/1988) et est appliquée depuis lors par les autorités compétentes.

3. En application de la directive 95/46/CE de l'UE, le flux transfrontière de données (principe 9) entre l'Autriche et les autres Etats membres de l'UE devrait être libéralisé prochainement.

4. Copie de la traduction officieuse de la loi sur la protection des données était jointe à la communication *.

Croatie

[Original : anglais]
[4 septembre 1996]

1. Le Gouvernement de la République de Croatie a procédé par l'intermédiaire de ses services compétents, à un examen attentif des Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, adoptés par l'Assemblée générale dans sa résolution 45/95, en vue d'en appliquer les dispositions au niveau national dans sa législation et dans la pratique.

2. A l'heure actuelle il n'existe pas de texte législatif général réglementant les fichiers informatisés contenant des données à caractère personnel. Les fichiers sont cependant réglementés par différents textes relatifs à des domaines particuliers de la vie publique où une protection des données à caractère personnel est nécessaire, notamment les affaires intérieures, la nationalité et la situation personnelle, les soins médicaux et, dans une certaine mesure, l'exécution des sanctions pénales. En outre, certains aspects de la réglementation des fichiers informatisés contenant des données à caractère personnel se trouvent dans les réglementations internes des divers organismes d'Etat ou publics s'occupant des domaines susmentionnés.

3. Un texte législatif général visant à réglementer les fichiers informatisés contenant des données à caractère personnel est actuellement en cours d'élaboration et devrait être soumis au Parlement au cours de l'automne 1996.

4. Pour l'établissement de ce projet, plusieurs instruments internationaux ont été pris comme modèles, en particulier la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, les Principes directeurs des Nations Unies

---

*Le texte peut être consulté au secrétariat.

précités et la directive la plus récente de l'Union européenne sur ce sujet (1996). Il a de plus été tenu compte des lois nationales adoptées récemment par plusieurs pays européens.

5. Lorsqu'il aura été adopté, ce texte contribuera certainement à renforcer la protection des fichiers informatisés contenant des données à caractère personnel et à harmoniser les normes applicables à leur utilisation.

Estonie

[Original : anglais]
[10 septembre 1996]

Les autorités compétentes de l'Estonie estiment que les Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel sont parfaitement raisonnables et applicables.

Jamahiriya arabe libyenne

[Original : arabe]
[2 octobre 1996]

1. La Jamahiriya arabe libyenne a examiné le projet de principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, mentionné dans la résolution 44/132 de l'Assemblée générale, qui met l'accent sur la nécessité de respecter les droits de l'homme et les libertés fondamentales des individus. Affirmant son adhésion à ces principes qui s'accordent avec sa politique systématique de défense de la liberté et de protection des droits des êtres humains où qu'ils se trouvent, et en conformité avec sa législation laquelle repose sur les préceptes du Saint Coran qui révère la personne humaine en tant qu'elle représente Dieu sur la Terre, et se fondant en particulier sur le grand document vert sur les droits de l'homme, elle a inscrit ses convictions en la matière dans la loi No 4 de 1990 sur l'information relative au système national de données de documentation, dont l'article 6 traite des données à caractère personnel de manière pleinement compatible avec les principes directeurs susmentionnés.

Article 6 de la loi sur l'information

2. L'utilisation de tout moyen coercitif ou frauduleux pour recueillir des informations ou des données à caractère personnel dans le cadre du Système national d'information est interdite. La personne concernée a le droit de prendre connaissance de ces informations et de ces données et de faire supprimer ou rectifier toutes celles qui, à son avis, sont en contradiction avec les faits réels avant qu'elles ne prennent valeur de document.

3. Ces données ou informations sont exclusivement utilisées aux fins de réaliser des études économiques et sociales. Aucun tiers, même s'il s'agit d'une autorité publique, n'est autorisé à y accéder et elles ne peuvent être diffusées d'une manière qui indique l'identité des personnes concernées, ni utilisées dans un autre but ou reconnues comme preuve ou justification pour une action en justice en contravention aux prescriptions susmentionnées.

4. On notera que les principes suivants sont inscrits dans cet article de la loi :

1. Licéité et loyauté dans la collecte des données à caractère personnel.

2. Vérification de la fiabilité et de l'exactitude des données à caractère personnel.

3. Finalité de la collecte des données.

4. Accès des personnes concernées aux dossiers contenant des données à leur sujet.

5. Non-discrimination, que l'article prévoit implicitement en interdisant de diffuser ou d'utiliser les informations à des fins autres que celles autorisées par la loi pour donner des indications sur l'identité des personnes concernées ou la révéler.

5. Les autres principes directeurs ayant trait à la sécurité, au contrôle et aux sanctions sont énoncés aux articles 7, 8 et 9 de la loi sur l'information.

6. La Jamahiriya a ainsi adopté ces principes qu'elle considère comme les garanties minimales à offrir pour sauvegarder les droits fondamentaux de l'homme.

Luxembourg

[Original : français]
[22 août 1996]

1. La loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques est conforme 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, sauf en ce qui concerne les principes 8 (contrôle et sanctions) et 9 (flux transfrontières de données), dont les dispositions ne sont pas expressément reprises dans notre législation.

2. Ces principes seront retenus par une nouvelle loi luxembourgeoise en matière de protection des personnes à l'égard du traitement de leurs données à caractère personnel, loi qui transposera en droit national les dispositions de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, transposition qui doit avoir lieu à l'issue d'une période de trois ans à compter de l'adoption de la directive.

Maurice

[Original : anglais]
[10 septembre 1996]

Le Gouvernement mauricien déposera prochainement un projet de loi sur la technologie de l'information (diverses dispositions) traitant entre autres des infractions dans le domaine de la protection des données, de la sécurité des données et de l'utilisation abusive des ordinateurs.

Mexique

[Original : espagnol]
[21 octobre 1996]

Principe de licéité et de loyauté

1. En ce qui concerne ce principe, le Registre national de la population et de l'identification personnelle est régi par la loi générale sur la population et, conformément aux dispositions de l'article 87 de cette loi, permet l'enregistrement des Mexicains sur le Registre national des citoyens, le Registre national des mineurs et le Rôle des Mexicains résidant à l'étranger ainsi que l'enregistrement des étrangers sur la Liste des étrangers résidant dans la République mexicaine.

2. Pour l'instant, tous les efforts sont consacrés à l'établissement du Registre des mineurs, qui est fondé sur les renseignements contenus dans les actes de naissance tirés des registres de l'état civil de la République à partir de 1982, conformément aux dispositions de l'article 89 de la loi susmentionnée.

3. Les registres d'état civil sont régis par les lois adoptées par les assemblées locales, qui définissent les diverses modalités d'inscription à respecter pour se conformer au principe de légalité et déterminent les mesures à prendre pour appliquer le principe de licéité et de loyauté.

Principe d'exactitude

4. Aux fins du Registre national de la population et de l'identification personnelle, il est obligatoire de vérifier l'exactitude et la pertinence des données enregistrées en validant les domaines d'information de façon à éviter les erreurs de numérisation ou bien des domaines d'information obligatoires pris en compte afin d'éviter toute omission de données importantes.

Principe de finalité

5. La loi susmentionnée est conforme à ce principe. En effet, même si pour l'instant seul le Registre des mineurs est en cause, l'article 86 de cette loi dispose que le Registre national de la population et de l'identification personnelle vise à enregistrer chacune des personnes formant la population du pays avec les données qui permettent de certifier ou de confirmer de manière

probante son identité. Cet enregistrement doit permettre de délivrer ultérieurement la carte nationale d'identité qui sera la pièce d'identité officielle prouvant en bonne et due forme les données relatives à l'identité de son titulaire qui y seront mentionnées.

6. Etant donné que l'acte de naissance ou la carte de naturalisation, en tant que certificat de nationalité, est indispensable pour enregistrer les personnes, la législation applicable au Registre d'état civil prévoit que ce dernier est public de façon à ce que toute personne puisse demander une attestation des faits qui y sont consignés.

7. On estime cependant que seul l'intéressé ou une autorité judiciaire peut avoir accès aux informations contenues dans le Registre national de la population et de l'identification personnelle. Lorsque la demande émane de l'intéressé, celui-ci doit, s'il est mineur, présenter une pièce d'identité et, s'il est majeur, sa carte nationale d'identité.

8. Quant à la conservation des données à caractère personnel, elle doit être permanente puisque ces données devront comprendre l'acte de décès, ce qui nous amène à une autre finalité du Registre, prévue à l'article 112 de la même loi, à savoir fournir à l'Institut électoral fédéral les renseignements contenus dans le Registre national des citoyens qui sont nécessaires pour l'établissement des liste électorales.

Principe de l'accès par les personnes concernées

9. En vertu du deuxième alinéa du paragraphe 1 de l'article 36 de la Constitution politique des Etats-Unis du Mexique, le Registre national des citoyens et la délivrance de la carte nationale d'identité sont des services d'intérêt public et, de ce fait, concernent l'Etat et les citoyens.

10. La loi générale sur la population régit la délivrance de la carte nationale d'identité et de la pièce d'identité des Mexicains âgés de moins de 18 ans. A ce titre, les intéressés ont accès aux informations pertinentes afin d'éviter l'enregistrement de données illicite, injustifié ou inexact. Toutefois, la loi ne prévoit pas de recours pour la rectification desdits enregistrements.

Principe de non-discrimination

11. Comme les informations destinées au Registre national de la population et de l'identification personnelle proviennent des actes du Registre d'état civil et que les lois applicables au Registre interdisent formellement l'enregistrement de données pouvant engendrer une discrimination illégitime ou arbitraire, il est impossible d'introduire dans la base de données une information ne figurant pas dans ces actes.

Faculté de dérogation

12. La publication des informations contenues dans la base de données du Registre national de la population et de l'identification personnelle est

prévue par l'article 112 de la loi générale sur la population, aux termes duquel les Services de l'intérieur fournissent à l'Institut électoral fédéral les données provenant du Registre national des citoyens qui sont nécessaires pour l'établissement des listes électorales.

Principe de sécurité

13. Pour protéger les fichiers contre les risques naturels, tels que la destruction par sinistre ou les autres risques mentionnés au point 7 des Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, le Registre national de la population et de l'identification personnelle protège les informations de sa base de données et les conserve dans un coffre-fort situé hors de ses locaux.

Contrôle et sanctions

14. L'article 113 de la loi générale sur la population définit les sanctions que les autorités des Services de l'intérieur, entité gouvernementale chargée de la base de données, en conformité avec le système juridique interne, peuvent appliquer aux employés qui enfreignent de diverses manières les dispositions en vigueur, par exemple communiquent des informations sur des questions à caractère confidentiel sans y être autorisés, entravent le déroulement normal des opérations par un acte frauduleux ou par une négligence grave, s'immiscent dans la gestion dûment réglementée de données ou accordent leur protection ou donnent des conseils, directement ou par personne interposée, pour éviter l'application de dispositions et échapper à des formalités.

Flux transfrontières de données

15. Les données destinées au Registre national de la population et de l'identification personnelle ne proviendront que des Mexicains résidant à l'étranger. Ils passeront cependant par les Services des relations extérieures, conformément à ce qui est prévu à l'article 96 de la loi générale sur la population.

Philippines

[Original : anglais]
[15 novembre 1996]

Le Gouvernement philippin a communiqué les documents suivants [*] fournis par la Commission de la fonction publique (CSC) des Philippines :

i) Règlement d'application du 21 avril 1989 relatif à la loi de la République No 6713 du 20 février 1989 intitulé "Code de conduite et principes de déontologie pour les fonctionnaires et employés de l'Etat";

[*] Les textes peuvent être consultés au secrétariat.

ii) Résolution No 92-1908 de la CSC, en date du 25 novembre 1992, intitulée "Précisions relatives à la loi sur la transparence en conformité avec la Constitution de 1987 et le Règlement d'application 6713";

iii) Mémorandum No 73 de la CSC, 1993.

L'information contenue dans ces documents complète le rapport sur l'application des principes directeurs présenté par le Gouvernement philippin le 22 septembre 1994 (E/CN.4/1995/75).

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

[Original : anglais]
[30 septembre 1996]

1. La législation britannique sur la protection des données prend en considération 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 au sujet desquelles des données font l'objet d'un traitement 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 réparation. Les détenteurs de données à caractère personnel informatisées doivent être inscrits au Registre de la protection des données (Data Protection Registrar) et respecter certaines règles spécifiées sur la manière dont ils obtiennent, enregistrent et utilisent leurs données.

2. Les éléments clefs de la loi de 1984 sont les suivants :

i) 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 législation de rendre publiques (par exemple les listes électorales), ou lorsque les données sont détenues pour des raisons de sécurité nationale (déterminées par les ministres du gouvernement);

ii) Tous les utilisateurs de données qui ne sont pas dispensés de cette obligation doivent déclarer le type de données qu'ils détiennent, les finalités en vue desquelles les données sont utilisées, 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;

iii) 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 par 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;

iv) 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 consignée au Registre) et un avis d'interdiction de transfert à l'étranger;

v) Les sujets fichés (les personnes physiques, non les organisations) peuvent demander réparation en justice pour les dommages causés par la perte, la destruction ou la divulgation non autorisée 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 la 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 à ces données risquerait de compromettre la prévention ou la détection d'un crime). L'intéressé 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;

vi) 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. Il 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;

vii) 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 l'intéressé);

viii) 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'usage. Il examine les plaintes pour violation des principes énoncés dans la loi et, le cas échéant, engage des poursuites ou émet des mises en demeure;

ix) 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 peut infirmer la décision du directeur du Registre. Les points de droit peuvent faire l'objet d'un nouvel appel devant la "High Court".

3. Le 3 février 1995, la loi sur la protection des données a été modifiée de façon à ériger en infraction le fait pour une personne, sachant ou fondée à penser que la divulgation de données à caractère personnel, d'obtenir la révélation de tels renseignements; et à ériger en infraction distincte la vente ou l'offre de vente par cette personne des données qu'elle s'est procurées. Cette disposition renforce la protection que la loi de 1984 assure à la sécurité des données personnelles. Elle a été introduite pour répondre aux inquiétudes suscitées par les activités de sociétés et d'agents d'enquête qui mettaient en vente des données confidentielles à caractère personnel (y compris des données d'ordre financier).

Saint-Marin

[Original : italien/anglais]
[5 et 11 septembre 1996]

1. En ce qui concerne la collecte informatisée de données confidentielles, la législation en vigueur dans la République de Saint-Marin se compose des lois No 70 du 23 mai 1995 (portant réforme de la loi No 27 du 1er mars 1983 réglementant la collecte informatisée des données personnelles) et No 71 du 23 mai 1995 ("Réglementation de la collecte de données statistiques et compétence administrative en matière de traitement des données"); cette dernière concerne plus spécifiquement le traitement des données au sein de l'Administration.

2. Cependant, il y avait déjà eu un début de réglementation en la matière. En particulier, la loi No 70 de 1995 abrogeait et remplaçait la loi No 27 du 1er mars 1983, à l'exception toutefois d'une série de décrets pris en Régence pour l'appliquer :

Décret No 7 du 13 mars 1984, "Création d'une banque publique de données, comme le prévoit l'article 5 de la loi No 27 du 1er mars 1983";

Décret No 7 du 3 juin 1986, "complétant le décret No 7 du 13 mars 1984 qui porte création d'une banque publique de données";

Décret No 140 du 26 novembre 1987, "Modalités à suivre pour la création des banques privées de données".

3. Le paragraphe II de l'article 20 de la loi 27/83 dispose clairement que ces décrets sont toujours en vigueur et sont compatibles avec la nouvelle réglementation.

4. La loi 70/95 joue un rôle plus important en ce qui concerne le point considéré. Elle a introduit dans le système juridique de Saint-Marin une série de principes généraux protégeant les fichiers contenant des données à caractère personnel. Après examen approfondi, ces principes ont été déclarés parfaitement conformes à ceux énoncés par la Commission des droits de l'homme, qui a établi une norme à laquelle devrait satisfaire toute réglementation nationale.

5. Le système juridique de Saint-Marin affirme les principes de licéité et de loyauté en interdisant expressément, au paragraphe I de l'article 7 de la loi 70/95, l'obtention de données personnelles et confidentielles par des moyens frauduleux, illicites ou déloyaux.

6. Les personnes chargées d'établir et de gérer les banques de données sont expressément priées de respecter les principes d'exactitude, de pertinence et de complétude, comme il découle clairement de l'article 14 de la loi 70/95 qui leur fait obligation de rectifier, de mettre à jour et de compléter de droit les données chaque fois qu'est relevée une information inexacte ou incomplète. L'article 14 dispose également que toute rectification, tout ajout et toute mise à jour sont notifiés gratuitement aux intéressés.

7. En ce qui concerne les raisons qui ont conduit à instituer un système de fichier informatisé, la législation en vigueur ne définit pas les objectifs spécifiques visés. On peut cependant les déduire de la procédure à suivre pour la création d'une banque de données, qui requiert l'autorisation préalable du Congrès d'Etat (gouvernement) et du Garant de la protection des données confidentielles et personnelles (art. 15). Ainsi, tout objectif spécifique motivant la création d'une banque de données est en définitive déclaré conjointement par ces organes. En outre, toute personne sollicitée en vue de la collecte de données à caractère personnel, destinées à être informatisées, doit être dûment informée des objectifs visés (art. 8). Il faut reconnaître que ce principe doit être encore précisé.

8. Inversement, le système juridique de Saint-Marin protège très efficacement le droit d'accès aux fichiers, dossiers et données à caractère confidentiel, dans la mesure où tout particulier a le droit de demander si des données personnelles le concernant ont été collectées ou traitées (art. 10) - et d'en obtenir copie (art. 11) - et aussi le droit d'exiger que des données inexactes, dépassées, incomplètes ou ambiguës, ou dont l'obtention, le traitement, la transmission ou la préservation sont interdites, soient rectifiées, complétées, précisées, mises à jour ou détruites (art. 12).

9. Dans tous les cas où il y a doute quant à la véracité et la conformité des données collectées et traitées, il est possible d'adresser une déclaration écrite au Garant, qui doit se prononcer dans un délai de 60 jours à compter de la réception de la déclaration sur la question de savoir si une enquête

administrative ou une intervention de la justice est nécessaire (art. 13); une requête peut être présentée en conséquence.

10. La loi 70/95 sanctionne pleinement le principe de non-discrimination, qui n'autorise la collecte d'informations spéciales qu'à condition que les intéressés y consentent, étant donné que ce type d'information (concernant, par exemple, les opinions ou activités politiques, syndicales ou religieuses) peut aboutir à une discrimination illégale ou arbitraire. En aucun cas la collecte d'informations de caractère extrêmement personnel n'est autorisée (art. 7).

11. Le principe de sécurité, en vertu duquel les mesures préventives appropriées doivent être prises pour éviter la destruction éventuelle de fichiers ou dossiers et pour prévenir l'accès non autorisé, est énoncé en termes généraux au paragraphe IV de l'article 4. Cet article dispose que le personnel d'une banque de données doit respecter rigoureusement le secret professionnel et prévoit des mesures propres à empêcher que l'information ne soit falsifiée, forgée de toutes pièces ou dévoilée à des personnes non autorisées.

12. S'agissant plus précisément du contrôle du respect effectif de ces principes, cette fonction incombe au Garant de la protection des données confidentielles et personnelles, qui est l'autorité compétente pour connaître de toute réclamation ou requête portant sur l'application de la loi susmentionnée et pour juger chaque fois qu'il est porté atteinte à la confidentialité des données à caractère personnel. Cependant, il est toujours possible d'en appeler à une juridiction supérieure, de droit commun ou administrative. Les autres fonctions du Garant sont aussi définies par la loi (art. 15 et 16). La façon dont cet office a été conçu répond pleinement à la nécessité de garantir l'impartialité et l'indépendance du personnel qui s'occupe d'informatiser les données confidentielles. Les fonctions de garant sont remplies par un juge du tribunal administratif.

13. Pour assurer la protection maximale des données confidentielles et une application plus efficace des lois pertinentes, l'infraction à certaines normes est passible de sanctions ou de mesures administratives (art. 17 et 18).

14. En ce qui concerne le transfert à l'étranger de données confidentielles concernant des Saint-Marininais, elle est soumise à l'autorisation préalable et motivée du Garant, qui devra vérifier si le pays auquel l'information confidentielle est communiquée assure le même niveau de protection des données personnelles que la législation saint-marinaise.

15. La loi 70/95 a un champ d'application vaste et général, puisqu'elle est applicable, sans distinction aucune, à tout système informatisé : fichier ou banque de données, du secteur privé comme du secteur public, propriété d'une personne physique ou d'une personne morale (art. 1er).

16. En conclusion, la législation en vigueur dans la République de Saint-Marin concernant la protection des données confidentielles et à caractère personnel est largement conforme aux principes énoncés par la Commission des droits de l'homme.

Suède

[Original : anglais]
[26 août 1996]

1. En août 1994, la Suède a présenté sur ce sujet un rapport (voir E/CN.4/1995/75) qui, à part certaines modifications, est toujours valable. Comme indiqué dans ce rapport, le gouvernement a présenté au Parlement, le 14 avril 1994, un projet de loi modifiant la loi sur la protection des données de 1973. Les amendements en question sont entrés en vigueur le 1er janvier 1995. Ils sont exposés dans le rapport de 1994.

2. Il faut cependant signaler une modification des amendements par rapport à ce qui est dit dans ce rapport : tous les appels de décisions de l'Agence de protection des données ne sont pas tous soumis à une instance judiciaire. Si le plaignant est une autorité publique relevant du gouvernement, c'est encore celui-ci qui connaît de l'appel.

3. Actuellement, sur le plan législatif, la principale question concernant la protection des données tourne autour de la nouvelle directive de l'Union européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (directive 95/46/EC). A compter de la date de son adoption, les Etats membres disposent d'une période de trois ans pour transposer la directive dans leur droit interne. Celle-ci a été adoptée le 24 octobre 1995.

4. Le gouvernement a institué une commission parlementaire spéciale pour rédiger une législation totalement nouvelle pour la protection des données dans le cadre de la directive de l'Union européenne. Il lui a notamment donné pour instruction de spécifier que la loi s'applique aux données à caractère personnel quel que soit le type de technique utilisé. La Commission terminera ses travaux avant la fin de mars 1997.

Uruguay

[Original : espagnol]
[11 juin 1996]

1. L'Etat uruguayen n'a pas encore mis en place de législation pénale spéciale pour réglementer le "crime informatique". La doctrine nationale n'en considère pas moins que les principes directeurs qui doivent régir l'utilisation des fichiers informatisés contenant des données à caractère personnel sont reconnus et protégés par la législation en vigueur.

2. Le droit uruguayen s'inscrit dans le cadre de la Constitution. Il convient donc de mettre en relief les dispositions suivantes :

> L'article 7, qui établit que les habitants de la République ont droit à la protection en ce qui concerne - entre autres - leur honneur, leur travail et leur propriété. Nul ne peut être privé de ces droits si ce n'est conformément aux lois établies pour des raisons d'intérêt général;

L'article 10, qui dispose qu'aucun habitant ne peut être contraint à faire ce que la loi n'ordonne pas, ni ne peut être privé de ce qu'elle n'interdit pas;

L'article 32, selon lequel la propriété constitue un droit inviolable, mais soumis aux dispositions des lois établies pour des raisons d'intérêt général. Nul ne saurait être privé de son droit de propriété, sauf dans les cas de nécessité ou d'utilité publique établis par une loi et moyennant le versement préalable d'une juste indemnité par le Trésor public;

L'article 33, qui dispose que la loi reconnaît et protège le travail intellectuel, les droits de l'auteur, de l'inventeur et de l'artiste;

L'article 36, qui établit que chacun peut se livrer au travail, à l'industrie, au commerce, à la profession ou à toute autre activité licite, sous réserve des limitations d'intérêt général établies par les lois.

3. Il convient de signaler qu'outre les normes spécifiques précitées, l'article 72 dispose textuellement ce qui suit :

"La liste des droits, des devoirs et des garanties contenue dans la Constitution n'exclut pas ceux qui sont inhérents à la personne humaine ou dérivent de la forme républicaine de gouvernement."

4. De même, l'article 332 établit que :

"Les dispositions de la présente Constitution reconnaissant des droits de la personne ou attribuant des facultés et imposant des devoirs aux autorités publiques ne resteront pas sans effet faute de textes d'application correspondants; on se référera aux principes qui sous-tendent des lois similaires, aux principes généraux du droit et aux doctrines généralement admises."

5. Les normes mentionnées ci-dessus constituent un cadre conceptuel solide pour la protection des droits que l'on se propose de sauvegarder [1].

6. Il convient de signaler cependant qu'à défaut de normes juridiques concrètes réglementant telle ou telle question précise concernant des bases de données, il pourrait être fait usage du recours en amparo, comme le dispose la loi No 16011 du 19 décembre 1988. En effet, selon l'article premier de cette loi :

"Toute personne physique ou juridique, publique ou privée, peut introduire un recours en amparo contre tout acte, toute omission ou tout fait des autorités publiques ou semi-publiques, ainsi que de particuliers qui, à son avis, est de nature, dans la réalité présente

---

[1] Mario Barreto Gugelheim "Protección jurídica de la base de datos", in La Justicia Uruguaya, tome 108, 1994, p. 41 à 50.

ou dans un avenir imminent, à léser, restreindre, altérer ou menacer, de façon manifestement illégitime, l'un quelconque de ses droits et libertés reconnus expressément ou implicitement par la Constitution (art. 72), à l'exception des cas où s'applique le recours d'" habeas corpus " [2].

7. En application de cette loi, le créateur intellectuel d'une base de données pourrait, par le biais du recours en amparo, intenter une action contre quiconque lèse, altère ou menace le droit consacré à l'article 33 de la Constitution, c'est-à-dire son travail intellectuel; ou encore, l'investisseur pourrait former ledit recours pour défendre son droit de propriété (art. 7, 32 et 36 de la Constitution); ou enfin, tout habitant pourrait défendre son droit à la vie privée - implicitement reconnu par l'article 72 de la Constitution - en faisant cesser l'omission ou le fait d'une autorité ou d'un particulier qui, selon lui, lèse, restreint ou altère les données à caractère personnel le concernant, ou risque de conduire à leur divulgation, leur mauvais usage ou la modification de leur finalité [3].

8. Dans l'hypothèse de l'incorporation dolosive d'informations inexactes dans les fichiers concernant des personnes, on peut envisager les mesures à prendre à la lumière des dispositions de l'article 240 du Code pénal uruguayen selon lequel :

"Quiconque fabrique un faux document privé ou altère un document authentique est puni, lorsqu'il en fait usage, de 12 mois d'emprisonnement à cinq années de réclusion criminelle."

9. Dans les cas où le sujet actif de la falsification immatérielle est un fonctionnaire, l'article 238 du Code pénal peut s'appliquer. Cet article dispose ce qui suit :

"Tout fonctionnaire qui, dans l'exercice de ses fonctions, confirmerait l'occurrence de faits imaginaires, ou de faits réels mais en en modifiant les circonstances, ou en omettant, modifiant ou supprimant les déclarations faites en la matière, est puni de deux à huit ans de réclusion criminelle."

10. Quant au respect dû au principe de finalité, la divulgation non justifiée de données personnelles est pénalisée en application des articles 301 et 302 du Code pénal selon lesquels :

"Article 301. Quiconque révèle sans justification le contenu des documents (publics ou privés) visés à l'article précédent qui serait venu à sa connaissance par les moyens énoncés dans ledit article ou

---

[2] N. Bergstein "Derecho penal e informática", in La Justicia Uruguaya , tome 111, 1995, p. 43 et suiv.

[3] Mario Barreto Gugelheim "Protección jurídica de la base de datos", in La Justicia Uruguaya , tome 108, 1994, p. 41 à 50.

d'une autre façon délictueuse, est puni de trois mois de prison à 3 ans de réclusion criminelle."

"Article 302. Quiconque révèle, sans justification, des secrets qui seraient venus à sa connaissance du fait de sa profession, de son emploi ou des tâches qui lui sont confiées est puni, lorsque le fait cause un préjudice, d'une amende de 100 à 2 000 pesos."
