COMMISSION DE LA
PROTECTION DE LA VIE PRIVEE

AVIS N° 34 / 98 du 14 décembre 1998

N. Réf. : A / 98 / 025 / 33

OBJET : Examen du caractère adéquat ou non du niveau de protection offert par le "Privacy Act" américain de 1974, conformément à l'article 25 de la directive 95/46/CE.

La Commission de la protection de la vie privée,

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier l'article 29;

Vu la demande d'avis du Ministre de la Justice du 8 octobre 1998;

Vu le rapport de M. Poullet;

Emet, le 14 décembre 1998, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS :

L'objet de l'avis porte sur le caractère adéquat ou non, de la protection offerte par la loi dite "Privacy Act" de 1974 au sens de l'article 25 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 (ci-après, la directive 95/46/CE).
Il s'agit ainsi de déterminer si des données à caractère personnel peuvent être transférées à des autorités américaines se prévalant de la protection accordée par le "Privacy Act".
Rappelons que le présent avis doit se lire conjointement avec les deux autres avis sollicités par le Ministre de la Justice à propos de la protection offerte aux données à caractère personnel aux Etats-Unis; le premier à propos de certains traitements du secteur du crédit, soit la protection offerte par le "Fair Credit Reporting Act", le second, à propos des traitements du secteur privé en général, soit la protection offerte par un document récent de l'Administration américaine (U.S. Department of commerce) intitulé "Elements of effective self regulation for privacy protection".

II. ANALYSE :

---

1. La Commission rappelle que l'examen proposé par l'article 25 de la directive 95/46/CE doit s'opérer non seulement au regard des principes de celle-ci mais également au regard des dispositions prises en Belgique en application de tels principes.
A ce stade, cependant, la Commission se bornera à appliquer les critères dégagés par le Groupe des représentants des Etats membres institué par l'article 29 de la directive et repris dans le document de travail adopté le 24 juillet 1998, intitulé "Transferts de données personnelles vers des pays tiers, application des articles 25 et 26 de la directive relative à la protection des données"[1] (ci-après, le document de travail européen).

2. Le "Privacy Act" de 1974 offre une protection sectorielle, c'est-à-dire qu'il institue une réglementation de protection des données pour la seule administration publique, c'est-à-dire les "agencies" selon le terme de la loi (Sec.552 a(1)). On note d'emblée que cette protection n'est valable que pour les citoyens des Etats-Unis ou des étrangers résidant légalement aux
Etats-Unis "lawfully admitted permanent residence" (Sec.552 a(2)). En d'autres termes, sauf modification de la loi ou engagement de réciprocité, les données relatives à des citoyens européens ne sont pas protégées. Dès lors, il va de soi que le "Privacy Act" américain n'offre pas une protection adéquate au sens de l'article 25, sauf si les données transférées d'Europe concernent des citoyens ou résidents permanents américains par exemple travaillant temporairement ou définitivement en Europe ou y voyageant. Cependant, ces flux ne représentent qu'une partie infime des flux de données à caractère personnel en provenance d'Europe vers les Etats-Unis. Il s'agira, le plus souvent de transférer des données concernant des personnes non protégées par le "Privacy Act".

[1](XV D/5025/98 - WP.12)

Nonobstant cette constatation liminaire et dans la perspective d'une éventuelle extension au bénéfice de la loi, la Commission a analysé le contenu de la protection offerte par le "Privacy Act", au regard des critères développés par le groupe institué par l'article 29 de la directive 95/46/CE. Elle s'en est tenue aux dispositions générales du "Privacy Act" et passe sous silence nombre d'observations qui auraient pu être formulées en ce qui concerne des traitements particuliers (sécurité sociale, sûreté de l'Etat,...) visés par la loi américaine.

3. En ce qui concerne le champ d'application du "Privacy Act", la Commission note que la notion de "record" est à la fois plus large et plus étroite que la notion européenne de traitement.
Plus large, dans la mesure où la notion de traitement fait référence dans la directive à une structure de données permettant une consultation systématique de celles-ci, alors que celle de "record" (Sec. 552 a (a) 1) désigne tout document, dossier reprenant des informations relatives à un individu. Par contre, il ne va pas de soi que soient couvertes toutes les données permettant indirectement l'identification de la personne, même si certaines de ces données sont couvertes ("identifying number, symbol or other identifying particular assigned to the individual such as a finger or voice print or a photograph").

4. En ce qui concerne les principes relatifs au contenu proposés par le Groupe de l'article 29, à savoir la limitation à une finalité spécifique, la qualité et la proportionnalité des données, la transparence, la sécurité, le droit d'accès, de rectification et d'opposition et, enfin, la restriction aux transferts ultérieurs, la Commission remarque que:

a) Le "Privacy Act" limite le droit des "agencies" à traiter les données aux seuls "routine uses" à savoir les buts compatibles avec les finalités pour lesquelles la donnée a été collectée, c'est-à-dire ceux fixés par "Statutes" ou par "Executive order" du "Statute President". La Commission note en outre que toute interconnexion de traitements est sévèrement réglementée (Sec 552. (a) 0): obligation de consigner par écrit les caractéristiques de l'interconnexion, description du but et la justification de celle-ci, analyse de l'impact de la connexion des traitements sur la vie privée et des avantages économiques escomptés de cette connexion de fichiers, procédure de vérification par un "Data Integrity Board" et publication préalable pour avis et réaction de la population. Au-delà du problème spécifique de l'interconnexion des fichiers, le point (6) de la Sect. 552 (a) affirme que la communication ("disclosure") entre administrations de données à caractère personnel, peu importe la technique, ne peut avoir lieu (sauf exceptions: sûreté de l'Etat, police) que moyennant l'accord de l'intéressé, à sa demande, ou si la communication est strictement nécessitée par l'exécution d'un "routine use" pour des find de recherche, et dans ce dernier cas, à condition d'une garantie écrite donnée par l'administration et l'anonymisation des données. Ainsi, le principe de finalité légitime apparaît parfaitement respecté.

b) Le principe de l'exactitude et de la proportionnalité des données est développé par le "Privacy Act". La Sect 552. a (c) oblige chaque administration, d'une part, à ne "maintenir" (collecter, traiter et communiquer) que les données "relevant and necessary" (pertinentes et nécessaires) et, d'autre part, à prévoir des procédures telles que les opérations sur les données assurant l'exactitude, "le routine use", la mise à jour et le caractère complet des données pour garantir un traitement équitable et loyal ("fairness") des personnes (Sect 552. a (c) 5). Ces procédures et leur respect sont examinés par le "Data Integrity Board".

c) La transparence vis-à-vis des personnes est largement assurée, de même que les droits d'accès, de rectification et d'opposition:

- La transparence est à la fois collective et individuelle. Une publication de tous les traitements ("system of records") et des projets d'interconnexion (cf. supra a) dans le "Federal Register" est exigée.
Par ailleurs, le principe de la collecte, dans toute la mesure du possible auprès de la personne concernée apparaît comme un bon principe (Sect 552. a(c) /2).
Enfin, l'information de chaque individu auprès duquel la collecte est effectuée, information figurant sur le document de collecte en annexe ou annexée à lui, porte sur l'autorité en charge du traitement, les finalités, et le cas échéant, les effets possibles du traitement pour la personne concernée.

- Les droits d'accès et de rectification font l'objet d'une procédure prévue à la Sect. 552 a (b) (2) (3) (4) (5). On retient les éléments suivants:
  - accès de la personne concernée "accompagnée", le cas échéant: cet accès s'opère vis-a-vis de l'ensemble des données (sauf exception pour certains types de traitements dans la mesure où une restriction d'accès est justifiée par un intérêt prédominant);
  - obligation de réagir pour une administration dans les dix jours ouvrables;
  - en cas de refus de modification de données, possibilité pour le citoyen de demander une révision de cette décision;
  - obligation de réagir pour l'administration dans les 30 jours;
  - obligation d'indiquer la contestation et la "portion" du traitement contestée lors des utilisations ultérieures;
  - droit du citoyen d'ester en justice.

d) La sécurité des données fait l'objet d'une attention particulière:
- obligation à charge de chaque "agency" d'adopter des "rules of conduct" pour les personnes concernées par la collecte des données, les développements et la maintenance des systèmes d'informations et de prévoir des sanctions en cas de non-respect;
- obligations de prendre les mesures de sécurité techniques, administratives et physiques pour garantir la confidentialité des données et leur sécurité;
- enfin, règles spécifiques pour tous les "Government contractors", sous-traitants de l'administration.

e) Les restrictions aux transferts des données vers les pays tiers découlent naturellement des considérations précédentes mais ne sont pas explicitement abordées.

5. Le document de travail européen qui fixe les critères de l'adéquation insiste sur la nécessité de prévoir, outre l'affirmation des principes développés ci-dessus, des mécanismes de procédure qui permettent d'assurer leur effectivité.

Les mécanismes de procédures poursuivent, suivant le document de travail, trois objectifs:

- *assurer un niveau satisfaisant de respect des règles.* Pour ce faire, l'existence de sanctions efficaces et dissuasives et la mise en place de systèmes de vérification sont importants pour ce faire;
- *apporter soutien et assistance aux personnes concernées dans l'exercice de leurs droits*. La personne doit être en mesure de faire valoir ses droits rapidement et efficacement sans avoir à subir des coûts prohibitifs. Pour ce faire, il faut mettre en place une sorte de mécanisme institutionnel permettant l'instruction des plaintes par une instance indépendante;
- *fournir des voies de recours appropriées,* ce qui requiert l'existence d'une institution d'arbitrage indépendante.

A la lecture du "Privacy Act", quelques réflexions peuvent être faites quant au respect de ces objectifs:

- Des mécanismes variés et effectifs de vérification a priori et a posteriori de la compatibilité des traitements avec les principes de la protection des données existent, mais de manière limitée.
En particulier, les interconnexions de traitements font l'objet d'une procédure de publicité et de vérification a priori, garantie par l'intervention d'un "Data Integrity Board" (Sect. 552 a (a)) qui recevra un dossier détaillé. Ces "Data Integrity Boards", créés dans chaque administration, exercent de multiples compétences de contrôle vis-à-vis de l'ensemble des communications d'informations entre administrations et publient un rapport annuel en la matière.
La mission du "Data Integrity Board" est explicitement la vérification des principes de protection des données lors de la transmission d'informations. On regrette que sa compétence ne soit pas étendue au contrôle des traitements purement internes de l'administration et que sa composition ne lui garantisse pas une complète indépendance. Il est en effet composé de "Senior officials designated by the head of the Agency".

En dehors de ce cas spécifique des communications d'informations entre administrations, on note la nécessité pour les administrations de publier leurs "routine uses" et les caractéristiques de leurs traitements (cf. point 6 c). De même tout projet de modification substantielle de leurs traitements fait l'objet d'un double envoi à une Commission du législatif, d'une part, et à l'"Office of Management and Budget", d'autre part, "in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals". Le mécanisme ne prévoit pas l'intervention d'une autorité indépendante. On ajoutera, à cet égard, que l'embryon d'autorité indépendante créé en 1974, la "Privacy Study Commission", a été dissout en 1977.

- Le soutien et une assistance des personnes concernées dans l'exercice de leurs droits ne font l'objet d'aucune disposition, même si la loi organise de manière efficace le recours contre l'administration. A cet égard, la loi ne prévoit aucun mécanisme institutionnel particulier pour l'instruction de plaintes par une autorité indépendante.

- Il convient de souligner que les "Data Integrity Boards", à supposer -*quod non*- leur indépendance ne peuvent être saisis par des particuliers et que la seule voie de recours est la voie judiciaire classique.

III. CONCLUSIONS :

Sur la base des considérations précédentes, la Commission estime:

- que le "Privacy Act" de 1974, bien qu'il présente d'incontestables mérites sur certains points, ne peut offrir une protection adéquate aux citoyens européens, en particulier en l'absence d'intervention d'une autorité de contrôle indépendante, chargée de contrôler le respect des principes et d'apporter soutien et assistance aux personnes concernées;

- que nonobstant ce fait, il est de son devoir d'attirer l'attention du gouvernement belge sur l'intérêt d'introduire dans notre législation certaines dispositions parallèles à celles proposées par la loi américaine, en particulier, celles relatives aux procédures, d'une part, mises en place lors de projets de connexions de fichiers ou d'extension de traitement, d'autre part, celles de fixation de règles de sécurité et de procédures efficaces lors de demandes d'accès ou de rectification de données.

Le secrétaire, Le président,

(sé) M-H. Boulanger. (sé) P. Thomas.