Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Droits et devoirs du ficheur

Poullet, Yves

Published in:
Welke commissie voor welke persoonlijke levensfeer = Quelles Commission pour quelle vie privée, actes juridiques de la journée d'information

Publication date:
1993

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 1993, Droits et devoirs du ficheur. Dans *Welke commissie voor welke persoonlijke levensfeer = Quelles Commission pour quelle vie privée, actes juridiques de la journée d'information.* Commission de la vie privée, Bruxelles, p. 47-70.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 16. Apr. 2024

beaucoup d'entre nous ont de la peine à comprendre. Les citoyens, fichés et numérotés, ont le sentiment d'être manipulés dans l'ombre, mais sont contraints de s'en remettre aux experts et aux autorités, du soin de protéger leur vie privée, dont la définition demeure introuvable. Il y a là des graves défis à la démocratie. La démocratie est fondée sur le débat, l'information, la responsabilité, et l'autodétermination des individus. Pas plus que l'on ne peut s'accommoder longtemps de la démocratie triste et indolente qui est un peu la nôtre, on ne conçoit pas une démocratie électronique ou une gestion automatisée de la démocratie. On n'y est pas encore, mais qui pourrait aujourd'hui dessiner le paysage de la société informatique dans vingt ans ? Il importe autant de démystifier l'informatique que de rendre les citoyens conscients des enjeux et des risques de l'informatique, de les informer complètement sur leurs droits et les moyens de les sauvegarder.

DROITS ET DEVOIRS DU FICHEUR

par Y. Poullet,,
Doyen de la Faculté de Droit aux F.U.N.D.P.
à Namur,
Directeur du Centre de Recherches
"Informatique et Droit" à Namur,
Membre de la Commission.

LE DROIT A L'INFORMATION DES ENTREPRISES ET DES ADMINISTRATIONS

FONDEMENTS, LIMITES ET CONDITIONS

INTRODUCTION

1. A partir de l'examen des dispositions de la loi belge récente du 8 décembre, enrichi par quelques réflexions de droit comparé et européen, la présente réflexion propose :

- une analyse du fondement même de droit à l'information des "ficheurs" dont découle une distinction a priori entre divers types de "ficheurs"* (Chap. I);

- l'examen du principe de finalité, conséquence même du fondement du droit à l'information des "ficheurs" et les diverses acceptations de ce terme de même que leur traduction légale (Chap. II);

- une réflexion sur les obligations légales diverses mises à charge du fichier (Chap. III).

* Par ficheur nous entendons l'ensemble des institutions, personnes physiques ou morales; privées ou publiques, qui entreprennent de collecter, traiter, diffuser ou communiquer des données nominatives, le lecteur excusera le néologisme qui ne peut être interprété comme péjoratif à l'endroit de telles activités.

CHAPITRE I. - DU DROIT A L'INFORMATION DES FICHEURS AUX DIFFERENTES CATEGORIES DE FICHEURS

I. Le "droit à l'information" des ficheurs comme notion fondamentale

2. Le "droit à l'information" des "ficheurs"... l'expression surprendra peut être. Un récent projet italien sur la protection des données en consacrait l'existence légale. A raison, car elle nous apparait être la conséquence indubitable de la liberté qui fonde la reconnaissance légale de l'activité des ficheurs privés, qu'il s'agisse de la liberté d'association dans le cadre de traitements opérés par un syndicat; de la liberté de culte à propos des traitements tenus par les autorités religieuses; de la liberté d'opinion lorsqu'il s'agit de traitements tenus par un individu pour ses besoins personnels; enfin, de la liberté d'entreprendre, liberté érigée dans notre pays au rang de liberté constitutionnelle, pour les multiples traitements opérés par les entreprises.

Dans le cas des administrations, ce droit découle de la poursuite par ces dernières de l'intérêt général. Comme le notait, dès 1983, le tribunal fédéral constitutionnel allemand (B. Verf. G., EUGRZ, 1983, 588), "la loi fondamentale résout la dichotomie individu - société en considérant la personne comme une entité liée et insérée dans la société.... C'est pourquoi, en principe, l'individu doit accepter des restrictions de son "droit à l'autodétermination en matière d'information" et ce en faveur de l'intérêt public prépondérant".

En d'autres termes, le droit à l'information des "ficheurs" se justifie dans tous les cas soit par l'exercice d'une liberté garantie par le Droit soit par l'intérêt public. Que l'exercice de cette liberté ou de cet intérêt public rencontre, voire se confronte à l'exercice d'autres libertés, celles des fichés, est évident. Les législations de protection des libertés ont précisément pour objectif premier de mettre en place le cadre par lequel se résoudra ce conflit de libertés (LEONARD-POULLET).

II. Les différentes catégories de ficheurs

3. L'examen du fondement invoqué par chaque "ficheur" pour justifier son droit à l'information permet d'en distinguer différentes catégories. A cet égard, la comparaison de la loi belge avec le projet de directive européen, voire avec les modèles législatifs étrangers, permet d'adresser à la première quelques critiques et de suggérer quelques distinctions supplémentaires, peut être implicites mais qui auraient gagné à être mieux exprimées.

§ 1. Les catégories de ficheurs particuliers

A. Les traitements gérés par des personnes physiques destinés à un usage privé, familial ou domestique et conservant cette destination

4. C'est la première catégorie de "ficheurs" visés par l'article 3, § 1, de la loi, il s'agit de désigner les agendas personnels, les listes d'adresse que chaque individu se constitue pour lui-même dans le cadre de ses relations privées, pour les exempter de toute application de la loi. Non aperçue par les législations dites de première génération, cette catégorie exemptée figure, à peu près dans les mêmes termes, dans la loi hollandaise, anglaise et dans le projet de directive, comme une conséquence de la multiplication des ordinateurs personnels. L'exemption d'une telle catégorie se justifie aisément : il y aurait contradiction, au nom de la liberté d'autrui, à limiter ma propre liberté d'opinion, en d'autres termes à permettre, pour protéger autrui, un contrôle de ma liberté individuelle.

Les agendas personnels tenus par les employés des entreprises sur des ordinateurs dédicacés et sans connexion possible avec le système d'information de l'entreprise sont-ils des traitements à usage privé. On peut en douter même si les obligations administratives imposées par la loi (déclaration, obligation de prévenir les fichés) devraient leur être évitées et si le texte en distinguant usage privé et familial ou domestique, laisse place à une interprétation possible.

B. Les syndicats, mutuelles, associations philosophiques et religieuses et politiques

5. Evoquant la réglementation de certaines données dites sensibles, l'article 6 de la législation belge prévoit comme ses consoeurs étrangères (1) que l'interdiction a priori n'interdit pas à "une association de fait ou dotée de la personnalité juridique de tenir un fichier de ses propres membres". Ainsi, l'association philosophique, religieuse, mutualiste, syndicale, politique, etc... peut-elle justifier, précisément au nom même de la liberté d'association qui la fonde, non pas une restriction aux libertés individuelles mais leur exercice coordonné au sein de telles associations.

La dérogation est mesurée. Il ne s'agit pas cette fois d'exempter de la loi mais simplement de l'interdiction de traiter un type particulier de données dont l'utilisation peut a priori faire craindre dans le chef d'autres ficheurs une discrimination et, dès lors, la remise en cause d'une liberté fondamentale de l'individu, qu'elle soit celle d'opinion philosophique, religieuse, d'appartenance mutualiste, syndicale ou politique. Ainsi, de tels ficheurs restent tenus de l'application des autres dispositions de la loi, en particulier du respect du principe de finalité (cf. infra n° 12).

(1) La donnée mutualiste n'est pas évoquée dans les autres législations. Sans doute, ceci est-il dû aux particularités du système mutualiste belge, coloré à la fois politiquement et religieusement.

C. La presse

6. Notre législation ne contient aucune disposition dérogatoire relative aux traitements opérés par des entreprises de presse. L'examen des législations étrangères et du projet de directive invite cependant à leur accorder un régime particulier : "considérant, écrit le préambule (Considérant n° 18) du projet de directive, que le traitement de données à caractère personnel à des fins journalistes doit bénéficier des dérogations aux dispositions de la présente directive nécessaire à la conciliation des droits fondamentaux de la personne avec la liberté d'expression et notamment la liberté de recevoir ou de communiquer des informations...". En d'autres termes, un statut particulier doit être réservé aux traitements de la presse dans la mesure où la liberté qui fonde le droit à l'information de tels "ficheurs" justifie une prise de renseignements plus étendue, des méthodes de collecte plus discrètes, qu'à l'égard des autres ficheurs.

§ 2. La distinction autorité publique - secteur privé

A. Le constat

7. La loi belge, nonobstant les remarques de la Commission de Protection de la Vie privée, ne retient apparemment pas cette distinction pourtant fondamentale dans l'ensemble des législations qui nous entourent, à l'exception de celle anglo-saxonne et du projet de directive. Certes, cette distinction se retrouve en filigrane dans certaines dispositions relatives en particulier aux exceptions faites à l'obligation d'informer la personne concernée dès le premier enregistrement (art. 9).

La justification apportée par le Ministre belge est fondée tant sur la difficulté de distinguer les deux secteurs que sur l'exemple prochain de la directive européenne dont la dernière version ne reprend plus cette distinction. Si une telle justification est séduisante, elle n'est pourtant pas convaincante dans notre pays de droit constitutionnel fondé sur la séparation des pouvoirs.

B. La légitimité de la distinction

... l'autorité publique

8. Le droit de l'autorité publique à collecter les données, à les traiter, à les communiquer s'explique, avons-nous dit, non par une liberté fondamentale qui justifierait en soi ce droit, mais par la nécessité d'assurer l'intérêt public. C'est la reconnaissance de l'intérêt public qui autorise certaines restrictions aux libertés de chacun, à leur droit à l'autodétermination.

Selon l'arrêt de la Cour constitutionnelle allemande déjà citée, ces restrictions du droit à l'autodétermination nécessitent cependant un fondement légal conforme à la Constitution et leur énoncé doit respecter les principes de clarté des normes et de proportionnalité. En ce qui concerne le traitement électronique de l'information, cela signifie

concrètement que "face au danger déjà décrit de l'usage du traitement automatique de l'information, le législateur doit prendre de plus amples mesures qu'auparavant quant à l'organisation et à la procédure d'un traitement de données, et ce, afin d'empêcher toute violation du droit de la personne humaine (...)".

Le droit à l'information des autorités publiques, indispensable pour assurer un service public efficace, et les restrictions du droit à l'autodétermination qu'il implique ne peut s'exercer que dans le respect de trois principes, ceux de légalité, de spécialité et de proportionnalité. Ces trois principes ont la signification suivante :

- le "principe de légalité", d'une part, que la création d'un traitement dans le secteur public trouve un fondement dans le cadre des compétences légales reconnues à ces administrations par "un organe de type législatif, que ce soit au niveau fédéral, régional, communautaire, provincial ou communal" et, d'autre part, que cette création s'opère sous le contrôle du législatif, contrôle que ce dernier peut exercer par la Commission comme c'est le cas en France. Au-delà du problème des libertés individuelles, le principe de légalité permet de préserver l'équilibre des pouvoirs. L'utilisation croissante de l'informatisation dans le secteur public renforce en effet les pouvoirs d'action de l'exécutif et modifie l'équilibre des pouvoirs, garant institutionnel de la démocratie. Le rattachement de l'autorité de contrôle de protection des données au législatif et le large droit de saisine accordé au législatif auprès de cette autorité participent également au rééquilibrage des pouvoirs;

- le "principe de spécialité" exige que chaque autorité administrative ne puisse enregistrer des données que dans le cadre de la mission spécifique qui lui a été confiée;

- le "principe de proportionnalité" implique, quant à lui, que les traitements mis sur pied par l'autorité administrative au nom de l'intérêt général ou de la protection des intérêts des citoyens n'engendrent pas une restriction disproportionnée des libertés individuelles, en d'autres termes, qu'ils soient strictement nécessaires à l'accomplissement des missions légales. En toute hypothèse, l'autorité administrative doit choisir la voie la moins coûteuse en termes de restriction des libertés de l'administré.

Un exemple témoignera de l'intérêt de tels principes : l'administration des transports souhaite commercialiser les données de son registre de la circulation routière. Une telle commercialisation ressort-elle de ses missions légales (principe de légalité)? Si oui, quelle donnée peut-elle communiquer et à qui ? Estimer que la transmission des données peut permettre à chaque propriétaire de véhicule d'être mieux informé du marché automobile et des assurances qui accompagne l'utilisation d'un véhicule revient à légitimer la communication des données aux secteurs automobiles et des assurances.

Estimer que la transmission de données est nécessaire uniquement pour assurer la sécurité des usagers de la voie publique conduit à restreindre l'accès aux services de gendarmerie, de police, aux assu-

rances voire aux constructeurs automobiles lorsque ceux-ci doivent prévenir des vices de construction... (principe de spécialité).

Enfin, à supposer que l'on soit dans la seconde hypothèse, le principe de proportionnalité conduit à n'admettre de la part des secteurs automobiles et d'assurance que des interrogations non sur l'ensemble du fichier mais spécifique à tel véhicule ou à tel type de véhicule.

Les principes de spécialité et de proportionnalité ont pour conséquence qu'au sein des administrations : "Il faut veiller à ce que des traitements dont la collecte et l'utilisation poursuivent des finalités différentes ne soient pas interconnectés. Il faut s'assurer ensuite que chaque domaine distinct de l'activité de l'administration reste bien séparé et ce par une interdiction de communiquer entre ces secteurs d'activité : le pouvoir exécutif devrait ainsi veiller à créer des domaines informationnels cloisonnés (...). Le principe général de la séparation des pouvoirs serait en conséquence complété (à l'intérieur de l'administration) par une "séparation des pouvoirs en matière d'information" (H. BURKERT).

9. Une telle analyse permet de répondre aux objections ministérielles. Certes, il est clair que de plus en plus, le secteur public opère sur le marché comme un agent du secteur privé : qu'on songe à l'activité des banques publiques, des entreprises publiques autonomes ou aux multiples activités concurrentielles assumées par certaines administrations, mais ce fait suffit-il à exclure, qu'hormis dans le cadre de telles activités, le secteur public, lorsqu'il agit avec l'imperium de l'autorité publique, ne doive point obéir à des règles qui permettent aux citoyens d'être assurés que l'intérêt général ait été défini par les autorités constitutionnelles habilitées. On peut concevoir que dans des pays sans régime constitutionnel ou non marqué par la séparation des pouvoirs, comme le Royaume-Uni (mais non les Etats-Unis), ces garanties existent par d'autres voies.

On concèdera dès lors que le projet de directive européenne ait dû, communauté oblige, ne pas heurter les traditions britanniques mais de là à abandonner la distinction dans un pays comme le nôtre présente un risque de dérive.

Tout traitement dans l'administration ne devrait-il pas être créé sous le contrôle de la loi ? L'exemple des législations hollandaise, allemande, française et américaine pour n'en citer que quelques-unes invite à cette conclusion. Il ne s'agit pas affirmer que de tels traitements recèlent un danger supérieur à ceux du secteur concurrentiel mais d'exprimer les conséquences mêmes du fondement de leur légitimité.

... le secteur concurrentiel

10. Dans le secteur privé, ou plus exactement au vu de ce que nous venons d'écrire, dans le secteur concurrentiel, le droit à l'information de l'entreprise se justifie par la liberté d'entreprendre.

Pour les entreprises offrant leurs services dans le cadre de relation contractuelle avec le fiché, "le service attendu de l'entreprise collectrice des données est à la fois la justification et la limite de l'usage des renseignements", concluait déjà le rapport Tricot, à la base de la loi française.

Certes, tel n'est pas le cas de toutes les entreprises en particulier celles nombreuses ayant pour mission au premier chef non de rendre un service au fiché mais bien à d'autres entreprises, ainsi les sociétés de services bureaux, les agences de renseignements commerciaux, les sociétés de mailing, etc.... Les lois allemandes, norvégiennes, danoises, autrichiennes leur réservent un statut particulier, plus contrôlé, à raison de leurs méthodes de collecte et de leur manque de transparence pour les fichés. Sans prévoir explicitement une catégorie particulière pour ces traitements, certaines dispositions de la loi belge les distinguent cependant. Ainsi, l'article 9 dispense d'information immédiate au premier enregistrement les responsables du fichier, traitant des données dans le cadre d'une relation contractuelle avec le fiché et ceux dont la relation est réglée par ou en vertu de la loi, mais non celles relevant de cette troisième catégorie.

Si la légitimité des traitements opérés par les entreprises relevant de cette troisième catégorie s'appuie également comme celle relative aux traitements opérés par les entreprises de la seconde catégorie sur leur liberté d'entreprendre, elle doit cependant être entourée de conditions particulières. En effet, l'appréciation de leur légitimité doit se faire au regard non de la relation qu'elles entretiennent avec le fiché mais bien du service, certes d'intérêt général incontestable (dépister les mauvais risques, permettre aux entreprises d'assurer la promotion de leurs produits ou de leurs services), qu'elles peuvent rendre aux entreprises qui recourent à leurs services. Nous reviendrons sur ce point lors de l'explicitation du principe de finalité.

CONCLUSION

11. Outre la création de catégories particulières de ficheurs, l'examen du fondement même du droit à l'information justifie la distinction entre les autorités publiques et les entreprises travaillant dans le secteur concurrentiel. Dans cette dernière catégorie, la réflexion invite à distinguer deux types de ficheur, ceux travaillant dans le cadre d'une relation directe avec le ficheur et ceux opérant pour compte d'autres entreprises.

De telles distinctions s'avèrent parfois délicates à tracer. En effet, de plus en plus, les administrations et sociétés exercent des activités multiples relevant des catégories diverses. Nous l'avons déjà dit à propos des administrations dont les fichiers servent à leur besoins propres mais sont, par ailleurs commercialisés (ficheurs opérant pour compte de tiers) ou dont les fichiers servent à la fois pour des opérations de service public et des opérations menées en concurrence avec des entreprises privées. Dans le secteur privé, la remarque s'impose plus encore, de nombreuses entreprises offrent des services contractuels variés à leur client, ainsi certaines banques offrent des services financiers et d'assurance, mais également deviennent des entreprises offrant à des tiers des services d'information ou de marketing.

CHAPITRE II. — LE PRINCIPE DE FINALITE : UN CONCEPT A MULTIPLES FACETTES

12. L'article 5 de la loi belge l'affirme de manière laconique : "les données à caractère personnel ne peuvent faire l'objet d'un traitement que pour des finalités déterminées et légitimes et ne peuvent pas être utilisées de manière incompatible avec ces finalités; elles doivent être adéquates, pertinentes et non excessives".

L'affirmation est neuve en Belgique : le projet Wathelet était le premier à reprendre explicitement ce principe pourtant pilier des législations de protection des données et la loi le consacre fort heureusement.

Le principe de finalité est essentiel. Les traitements de données présentent des risques non tant en fonction de la nature des données y reprises que par les finalités poursuivies. Ainsi, même la donnée religieuse peut figurer légitimement dans le traitement d'une compagnie aérienne pour les seuls besoins de la gestion des repas mais représente un risque de discrimination intolérable dans les traitements nécessaires à l'embauche du personnel.

13. On s'étonnera cependant de son peu d'explicitation. Le projet de directive européenne, mais déjà la convention du Conseil de l'Europe, introduisent en effet une réflexion sur les multiples facettes de ce principe. Ainsi l'article 6 du projet de directive évoque les principes relatifs à la "qualité" des données tandis que son article 7 détaille les divers "fondements" ou la "légitimité" des traitements. Ainsi se trouvent distinguées plus clairement (LEONARD - POULLET) deux notions fondamentales, selon nous : la légitimité des traitements et la conformité de leur contenu à cette légitimité.

Illustrons cette distinction par un exemple : une école secondaire souhaite commercialiser certains renseignements relatifs aux étudiants sortants. Elle s'interrogera successivement sur les points suivants :

- la légitimité du traitement en lui-même, c'est-à-dire de la commercialisation du fichier : l'école peut-elle communiquer des données sur les étudiants sortants ? A cet égard, elle s'interrogera sur la qualité des destinataires : la commercialisation a-t-elle lieu vis-à-vis d'institutions d'enseignement qui ont pour mission de prolonger la scolarité de ses étudiants ou a-t-elle lieu vis-à-vis de banques, de sociétés d'assurance ou d'agences de voyages, auxquels cas le lien avec le but initial de la collecte n'est pas aussi évident.

- la première question résolue, l'école s'interrogera sur la conformité du contenu pour chaque hypothèse de traitement légitime : à supposer que l'école estime que la communication est légitime. Reste à savoir les données susceptibles d'être transmises. S'agit-il de la simple liste alphabétique des étudiants (?) complétée de l'adresse (?), des résultats finaux (?), intermédiaires (?) des noms et de la profession des parents (?)...

Une trop large transmission risque d'être dangereuse pour l'étudiant. Pire, la conservation illimitée de certaines données (ex. : a réussi ses humanités en 7 ans) risque de figer l'image d'un étudiant et de le punir à tout jamais pour une erreur de jeunesse.

14. Que ce soit dans l'examen de la légitimité ou de la conformité, le "ficheur" a le droit de s'interroger sur les intérêts mis en cause par le traitement.

Le traitement des données à caractère personnel suscite une opposition d'intérêts entre les personnes concernées par les données et celles qui les traitent. La seule possibilité de circonscrire les limites de l'utilisation des données, concrétisées par les principes de légitimité et de conformité, est d'équilibrer les intérêts en conflit. Ces deux principes ont dès lors un même objectif : pondérer les intérêts.

Pondérer les intérêts est un exercice périlleux dès lors qu'aucune démarche systématique n'est proposée au juge ou à l'autorité de contrôle afin de guider leur raisonnement.

"Prôner la pondération des intérêts ne revient qu'à cerner le résultat à atteindre. Ce faisant, on ne rend pas compte du double contrôle préalable à toute recherche d'équilibre. Comment équilibrer deux libertés (intérêts, etc..) sans poser dès le départ la question du lien de causalité entre les moyens que l'on met en oeuvre et la liberté (ou l'intérêt) dont on prévaut ? Comment également ne pas vérifier si la restriction apportée à la liberté de la vie privée est réellement nécessaire à l'expression pleine et entière de la liberté ou de l'intérêt qui provoque cette atteinte (2) ?

Pareille absence de démarche logique et systématique garantissant formellement la validité de l'équilibre retenu comme solution, peut susciter un sentiment de méfiance par le trop grand pouvoir d'appréciation laissé à ceux qui ont pour mission de contrôler la correcte application du principe de finalité. On peut craindre en effet que, suivant l'humeur du moment, la pression des événements, le fléau de la balance penche tantôt à droite, tantôt à gauche. D'où le besoin de munir le juge et l'autorité de contrôle d'un certain nombre de critères qui leur permettent d'assurer, à la suite d'une démarche rationnelle, le respect d'un équilibre entre les libertés ou/et les intérêts en présence.

15. Afin de fixer les limites au pouvoir d'appréciation de ceux qui ont pour mission d'appliquer le principe de finalité, on peut, à la suite d'une réflexion de M. VAN GERVEN (3), tenter de rechercher l'équilibre des intérêts en appliquant la règle de proportionnalité. L'auteur a très bien montré comment celle-ci, utilisée depuis longtemps en droit économique européen, se retrouve mutatis mutandis dans la problématique de la protection des droits fondamentaux. Avant d'entrer plus avant dans l'argumentation, il convient de rappeler en quoi consiste la règle de proportionnalité.

---

(2) Le professeur RIGAUX relève d'ailleurs qu'aux Etats-Unis comme dans le système constitutionnel allemand, "l'atteinte portée à une liberté fondamentale doit être limitée à ce qui est strictement nécessaire, soit pour donner satisfaction à l'intérêt général, soit pour assurer la protection d'un intérêt privé".

(3) W. VAN GERVEN, "Principe de proportionnalité, abus de droit et droits fondamentaux", J.T., 1992, pp. 305 à 309.

L'application de la règle de proportionnalité implique un triple examen (4), qu'elle porte sur la légitimité d'une atteinte par un particulier à un droit ou une liberté d'autrui ou sur un acte déterminé pris dans l'exercice d'une compétence. Le premier concerne le contrôle de l'utilité de l'acte ou des moyens mis en oeuvre. Il s'agira de vérifier s'ils présentent un lien de causalité suffisant avec l'objectif poursuivi. Le second vise le caractère indispensable des mesures prises ou envisagées, eu égard au fait qu'elles ne peuvent être remplacées par d'autres mesures qui permettraient d'atteindre le même objectif avec une efficacité identique tout en étant plus respectueuses de la liberté, de l'intérêt ou du droit ainsi énervé. Le troisième s'assurera que l'atteinte aux libertés impliquée par les mesures prises n'est pas disproportionnée par rapport au but poursuivi" (LEONARD-POULLET).

16. L'exemple de la création au sein d'un groupement bancaire d'une liste des émetteurs de chèque sans provision peut illustrer notre propos. La nécessité de dépister les mauvais risques, c'est-à-dire les personnes ayant déjà émis des chèques sans provision justifiera certainement la création de ce traitement nouveau et permet de répondre positivement au premier examen. Le second examen révélera certainement qu'un accès non point total à la banque de données mais limité à l'interrogation à partir de noms précis est plus respectueux de la liberté d'autrui. Enfin, le traitement en question porterait atteinte disproportionnée aux intérêts du fiché si la durée de conversation des informations ainsi reprises n'était pas limitée.

I. La légitimité du traitement

17. Notre propos décrit dans un premier temps les caractéristiques dont la loi entoure l'affirmation du principe de finalité : la finalité d'un traitement doit être définie, légitime et transparente. L'énoncé de ce principe oblige à analyser deux questions particulières. Premièrement, dans quelle mesure, le consentement permet-il de déroger en particulier aux contraintes qu'impose la nécessité d'une légitimité du traitement ? En d'autres termes, le consentement permet-il de légitimer tout traitement ? Secondement, comment aborder la question délicate de la "communication ", c'est-à-dire du traitement constituant une utilisation externe des données collectées, qu'elles soit accessoire ou principale.

§ 1. Les principes

18. L'article 5 de la loi belge, comme l'article 5b de la Convention 108 du Conseil de l'Europe, parle de finalités déterminées et légitimes, l'article 6b du projet de directive ajoute : elles doivent être explicites. Ainsi, le principe de légitimité d'un traitement exige à la fois la spécification des buts poursuivis par celui-ci, leur légitimité et finalement leur transparence.

(4) Sur son application par la Cour de justice européenne, voir les conclusions de l'avocat général W. VAN GERVEN dans l'affaire Eurim-Pharma, C-347/89, Rec. p. 1760.

A. La spécificité

19. C'est dans la mesure ou les buts d'un traitement sont suffisamment précisés que les autorités de contrôle et le fiché lui-même pourront apprécier, sur base de l'énoncé de la finalité, dans quelle mesure l'obtention de telle ou telle donnée, est nécessaire, en d'autres termes de contrôler, dans un premier temps la légitimité du traitement, dans un second temps, la conformité aux buts du traitement. Ainsi, amènera-t-on l'assureur à distinguer plusieurs finalités chaque fois qu'il s'agira de polices de types distincts, le banquier à estimer que la finalité gestion des comptes-crédit est distincte de celle gestion des comptes courants, a fortiori, de celle "marketing de nouveaux produits" et de celle "polices d'assurances", lorsque la banque est également assureur.

La "gestion du personnel", finalité générique, recèle de multiples finalités spécifiques : assurer la paie des employés, remplir les obligations vis-à-vis des administrations de sécurité sociale, gérer la carrière des employés, contrôler l'utilisation des ressources communes de l'entreprise (par ex. utilisation du réseau téléphonique), les activités paraprofessionnelles, etc. Pour chacune de ces finalités, l'entreprise définira la nature des données nécessaires et les catégories d'utilisateurs. Cette obligation de spécifier chaque finalité n'implique pas l'énumération de chaque application (plusieurs applications concourant à assurer une même finalité spécifique : ainsi, un système d'aide à la décision peut faciliter l'utilisation de la banque de données où sont reprises les informations relatives à la carrière des employés); il n'est pas évident non plus qu'elle implique l'obligation administrative d'opérer une déclaration pour chaque finalité. La Commission pourrait parfaitement, comme c'est le cas au Royaume-Uni ou aux Pays-Bas, se contenter d'exiger une déclaration par finalité générique, étant entendu qu'à l'intérieur de cette déclaration sont spécifiées chacune des finalités déterminées.

B. La légitimité

20. L'article 7 du projet de directive évoque les diverses hypothèses de légitimité des traitements : les points a) relatif au consentement, et f), relatif à la communication, faisant l'objet de développements séparés, on notera en particulier les points b) et c). Le premier s'adresse de préférence au secteur privé ou concurrentiel, le traitement y est légitime lorsqu'il est nécessaire pour l'exécution du contrat passé avec la personne concernée ou pour l'exécution de mesures précontractuelles prises en réponse à la demande de celle-ci.

Le second s'applique en particulier aux traitements des autorités publiques; le traitement est alors légitime, s'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers à qui les données sont communiquées.

C. La transparence

21. L'exigence n'est pas reprise telle quelle à l'article 5 de la loi belge. Elle se déduit cependant aisément d'autres dispositions sur

lesquelles nous reviendrons (infra n° 27 et s.). Ainsi, lors de la collecte, les "buts" (il eût été préférable que le texte de la loi reprenne le terme "finalité") de la collecte et donc du traitement devront faire l'objet d'une information du fiché et, surtout, le registre tenu par le maître du fichier de même que sa déclaration énoncera les finalités du traitement.

§ 2. Légitimité et consentement

22. En dehors de ces deux hypothèses, le point a) de l'article 7 du projet de directive semble consacrer le principe suivant lequel le consentement de la personne concernée suffit à légitimer le traitement. Certes, il s'agit d'un consentement éclairé, susceptible d'être retiré à tout moment (art. 1g). La disposition sous-entend cependant qu'une entreprise puisse utiliser des données au-delà des buts contractuels qu'elle entretient avec le client et dès lors les communiquer à des tiers. On notera que la loi belge hormis le cas des données médicales (art. 7, alinéa 2) - ce qui est étonnant - n'a pas permis une telle souplesse craignant sans doute, que quoi qu'on en dise, dans les relations ficheur-fiché, le consentement ne soit jamais totalement libre et éclaire (RIGAUX).

Plus fondamentalement, on s'interroge : le consentement peut-il suffire à légitimer un traitement ?

Une réponse positive permettrait à une entreprise de poursuivre, étant donné le consentement du fiché, des buts injustifiables : la banque utiliserait les données collectées dans le cadre de son activité bancaire pour servir d'agence de renseignements sur la solvabilité, une administration fiscale forte du consentement du citoyen communiquerait les renseignements obtenus au mépris du secret administratif. Une telle conclusion apparaît intenable. Ce que l'on peut concevoir, c'est que le consentement permette à l'entreprise, à l'administration dans le cadre des finalités légitimes qui sont les leurs, d'élargir le nombre de données collectées, voire le nombre d'utilisations de ces données, bref, que les entreprises puissent déroger au principe de conformité mais non à celui de légitimité. Ainsi, pourrait-on admettre le traitement de certaines données sensibles ou de données non pertinentes a priori; en d'autres termes, est laissée à la Commission et au juge la possibilité d'exercer leur mission de contrôle de légitimité. Dès que le traitement des données nominatives ou les buts dans lesquels certains traitements sont effectués s'avèrent impliquer une ingérence inacceptable, fût-ce sous le couvert du consentement de la personne, l'autorité doit soit pouvoir frapper le traitement d'illégitimité, soit ordonner que des mesures particulières soient prises afin de rééquilibrer les intérêts en présence.

§ 3. Légitimité des traitements opérés pour compte de tiers et légitimité de la communication

23. Le point f) de l'article 7 du projet de directive concerne tant la légitimité des traitements opérés pour compte de tiers que celle de la communication. La notion de communication n'a pas été reprise en

droit belge malgré le désir répété de la Commission de protection de la vie privée. Elle se définit, au sens du projet, comme la transmission externe à des tiers, c'est-à-dire en dehors du cercle des utilisateurs qui peuvent se prévaloir d'une utilisation directement liée à la finalité d'un traitement et qui se trouvent dès lors placés sous l'autorité directe du responsable du fichier ou agissent pour son compte. Cette communication obéit à des conditions particulières : une telle transmission doit être nécessaire, dit le projet, à la poursuite de l'intérêt général, de l'intérêt légitime du responsable du traitement ou du ou des tiers auxquels les données sont communiquées, à condition que l'intérêt de la personne concernée ne prévale pas.

24. Le texte oblige dans les deux cas visés à envisager de multiples intérêts : celui général, celui légitime du responsable du traitement, celui du tiers et, finalement, celui de la personne concernée. Il s'agit, selon le texte, de constater la présence de deux des trois premiers et de le mettre en balance avec le dernier. Ainsi, dans le secteur bancaire, la communication d'un risque de crédit par la banque à l'assureur crédit répond à l'intérêt légitime du responsable du traitement et ne contrevient pas dans une mesure excessive à l'intérêt du client bancaire, si les données transmises sont utilisées dans le seul but d'apprécier le crédit demandé et non dans le but de les commercialiser.

Ainsi, la cession par la Poste d'un fichier reprenant la liste de personnes ayant déménagé répond certes à un intérêt légitime à la fois du responsable du traitement (la Poste) et des tiers à qui communication est faite. Cette cession pourrait cependant violer l'intérêt légitime de la personne concernée si une possibilité de s'opposer à la transmission de la donnée le concernant ne lui était pas offerte. Il s'agit, on le voit, d'arbitrer des conflits d'intérêts et, le cas échéant, de trouver, comme dans l'exemple de la Poste, des modalités permettant de les concilier. Rôle délicat qui sera celui non seulement des Commissions instituées à cet égard mais également des juges appelés en définitive à trancher les litiges.

Si la loi belge ne réglemente pas comme telle la communication à des tiers, on relève cependant la notion à de multiples reprises : la loi fait obligation (article 12, § 3) aux ficheurs de transmettre les corrections aux personnes ayant été destinataires de communication pendant les 12 derniers mois et l'article 21 permet "selon des modalités fixées par arrêté royal délibéré en Conseil des Ministres, sur proposition ou après avis de la Commission de Protection de la Vie privée" d'interdire ou de réglementer les rapprochements, interconnexions ou toute autre forme de mise en relation de données à caractère personnel faisant l'objet de traitements. Une telle disposition qui vise les transferts de fichiers, est maladroite. Un arrêté royal pourra-t-il envisager avec suffisamment de souplesse les multiples nuances auxquelles conduit l'examen du respect du principe de finalité énoncés ci-dessus ? Il ne pourra s'appliquer que dans des cas précis où de toute évidence, la communication de données présente des risques graves d'atteinte aux intérêts légitimes de fichés.

II. La conformité du traitement

25. L'analyse de l'article 6c, d) et e) du projet de directive conduit à reconnaître, à ce second principe, trois facettes déjà affirmées par la Convention du Conseil de l'Europe mais, me semble-t-il, non reprises intégralement par la loi belge : la pertinence, la qualité et les limites a la conservation des données.

§ 1. La pertinence

26. La première (article 6c) consacre que "les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées". Il s'agit de contrôler, selon la règle de proportionnalité, si les données collectées sont nécessaires à l'accomplissement des buts poursuivis par le traitement. L'enregistrement de résultats scolaires ou du nombre de domiciles est-il pertinent pour déterminer la solvabilité d'une personne dans le cadre d'un traitement tenu par une agence de renseignements commerciaux ? La réponse n'est pas nécessairement négative, ce sera à l'entreprise de démontrer le bien fondé de l'utilisation de tels critères, le jour où une personne concernée affirmera que de telles données doivent être effacées. Au juge de trancher alors.

En d'autres termes, la pertinence est un concept flou qui renvoie à une appréciation, a priori par l'entreprise elle-même de ses besoins, a posteriori, en cas de litige, par le juge. Qu'elle puisse, le cas échéant, se justifier est la seule contrainte que lui impose la règle de proportionnalité.

§ 2. La qualité des données

27. La deuxième exigence, déduite du principe de conformité, est celle de la qualité des données : celles-ci "doivent être exactes et, si nécessaire, mises à jour". Notre loi belge évoque indirectement cette obligation (car il s'agit d'une obligation cette fois !) à l'article 16, § 3° : "le maître du fichier... est tenu : .. 3°) de faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes ou non pertinentes... ". Le Ministre a pris soin de souligner qu'il s'agit là d'une obligation de moyens. Il ne peut être question de reprocher à un maître du fichier l'inexactitude d'une donnée mais d'apprécier si étant donné la nature du fichier et les conséquences d'une absence de qualité des données pour le fiché, le maître du fichier a pris les précautions raisonnables pour une mise à jour régulière de ses banques de données. Sur ce point, on imagine aisément que ne peuvent être traitées sur le même pied la Banque Nationale qui tient la liste des incidents de paiement, et une société de mailing.

§ 3. La durée de conservation

28. La troisième exigence vise la durée de conservation des données. Elle ne peut excéder la durée nécessaire à la réalisation des finalités poursuivies. Une telle disposition ne se retrouve pas explicitement dans la loi belge, comme le regrettait déjà la Commission à propos du projet de loi. L'instauration d'un "droit à l'oubli" est remarquable dans les législations des pays qui nous entourent. Ce droit se trouve parfois précisé. Ainsi, dans le domaine du crédit, la recommandation de la CNIL française du 30 avril 1985 relative à la gestion des crédits ou des prêts consentis à des personnes physique prévoit qu'en aucun cas la durée d'enregistrement des impayés "n'excède trois ans pour les dossiers qui ont été soldés et cinq ans pour les créances qui ont été passées en perte". Chez nous, la loi n'émet aucun principe général à ce propos (cf. cependant, infra n° 37 : à propos de la déclaration des traitements). Il s'agira dès lors de déduire du principe de finalité de l'article 5 ces limites à la conservation des données.

Conclusions

29. L'examen du principe de finalité amène le maître du fichier à se poser les questions suivantes :

- Quelle(s) raison(s) précise(s) justifie la création de traitements ?

- Ces raisons découlent-elles à suffisance pour les administrations de la mission légale qui leur est confiée ou peuvent-elles pour les entreprises se fonder sur les nécessités de la relation qu'elles entretiennent avec le fiché ?

- Les données collectées et traitées (données de base ou résultat) sont-elles dans leur nature et leur qualité strictement nécessaires à l'obtention des buts légitimes poursuivis ?

- Leur mise à jour est-elle opérée à des intervalles raisonnables ?

- La durée de conservation des données n'excède-t-elle pas les besoins découlant des nécessités à la base du traitement ?

30. Dans le secteur concurrentiel, la réflexion sur la signification du principe de finalité peut être menée de manière collective; au sein d'associations professionnelles. Le projet de directive, en ses articles 28 et s., reprend sur ce point le modèle hollandais, anglais et irlandais, des "codes de conduite" : "Les Etats membres peuvent prévoir que les codes de conduite élaborés par les milieux professionnels peuvent fixer des mesures complémentaires répondant aux spécificités de certains secteurs...". Le projet envisage en outre l'existence de codes de conduite communautaires et institue, d'une part, un contrôle par les autorités de protection des données, contrôle de fond après audition des parties intéressées (y compris donc des représentants des fichés) et de représentants de l'association qui a préparé le code et, d'autre part, la publication officielle des codes ayant reçu un avis favorable.

Sans doute, est-ce à la lumière de ce modèle qu'il faut comprendre l'article 44 de notre loi. "Le Roi peut, par arrêté délibéré en Conseil des Ministres, après avis de la Commission de Protection de la Vie Privée, préciser la mise en œuvre des dispositions contenues dans la

présente loi en vue de tenir compte de la spécificité des différents secteurs" ! On note que la loi belge introduit ainsi un troisième personnage dans le dialogue entre les associations professionnelles et l'autorité de protection des données et cela en consacrant par arrêté royal l'initiative privée, sans exiger par ailleurs, que le code de conduite constitue une amélioration de la protection offerte aux citoyens. La sanction royale ôte en outre aux codes de conduite la souplesse souhaitable vu l'évolution continue des technologies. Certes l'intérêt de la sanction royale se conçoit aisément : il s'agit de lever les incertitudes relatives à la valeur des codes de conduite qui pourraient n'être considérés que comme l'expression des règles de l'art sans lier le juge (BOULANGER - de TERWANGNE).

31. Le principe de finalité est le seul principe évoqué par la loi belge. La comparaison avec le projet de directive et la loi française justifie l'affirmation d'un autre principe : celui de la non suffisance du traitement ou, en termes plus positifs, le droit pour toute personne "de ne pas être soumise à une décision administrative ou privée lui faisant grief, prise sur le seul fondement d'un traitement automatisé qui définit un profil de personnalité". Il s'agit de condamner l'utilisation de l'outil informatique comme seul fondement d'une décision vis-à-vis de la personne concernée, en particulier les gestions automatiques de carrière ou le "crédit scoring".

CHAPITRE III. — LES OBLIGATIONS ACCESSOIRES DU FICHEUR

32. Deux obligations retiendront notre attention : la première, celle de la transparence, n'est qu'une des conséquences de l'obligation de rendre explicite la ou les finalité(s) du traitement. Cette obligation de transparence a une quadruple signification.

La seconde obligation est de définir les mesures de sécurité aptes à garantir la confidentialité des données.

I. Les obligations administratives assurant la transparence des traitements

33. La loi belge n'entend pas, hormis les traitements de données sensibles, les soumettre à autorisation préalable. C'est au maître du fichier de définir la finalité de ses traitements et à apprécier à la fois leur légitimité ainsi que la conformité de leur contenu aux exigences de cette légitimité. Si cette position ne surprend pas pour les traitements opérés par le secteur concurrentiel, elle est plus étonnante vis-à-vis des autorités publiques. Les pays qui nous entourent exigent en effet que la finalité des traitements soit définie par ou en vertu de la loi (cf. dans ce sens également nos réflexions supra chap. I.).

La législation distingue quatre étapes nécessaires à assurer la transparence des traitements : il s'agit d'abord d'une transparence interne à l'entreprise ou à l'administration, du système d'information dont elle dispose : le registre de l'article 16. De cette première mesure, l'article 17 distingue la transparence vis-à-vis de la Commission qui conduit à consacrer une obligation de déclaration. Cette déclaration permet à la Commission d'assurer, cette fois vis-à-vis du public, la transparence du fichier par la mise sur pied du registre public institué par l'article 18. Enfin, lors de la collecte de renseignements auprès du fiché, une obligation de fournir certains renseignements au fiché existera.

§ 1. Le registre de l'article 16 : la transparence interne

34. "Le maître du fichier... est tenu d'établir pour chaque traitement automatisé un état où sont consignés la nature des données traitées, les buts du traitement, les rapprochements, les interconnexions et les consultations, ainsi que les personnes et les catégories de personnes à qui les données à caractère personnel sont transmises".

Une telle obligation lui permettra de connaître les flux internes générés par le système d'informations mis en place et de réfléchir sur leur contenu, leur pourquoi et leurs destinataires. Une telle élucidation représente, de l'aveu même des entreprises, un intérêt direct pour elles-mêmes, obligées de s'interroger sur leurs pratiques, elles sont bien souvent amenées à constater la redondance voire l'inutilité de certaines informations, à préciser les destinataires de celles-ci et à entourer certains flux internes d'un minimum de protection.

§ 2. La transparence vis-à-vis de la Commission de Protection de la Vie privée : le régime de déclaration de l'article 17 de la loi

35. L'article 17 de la loi belge prévoit, préalablement à la mise en œuvre d'un traitement automatisé, sa déclaration par le maître du fichier. Ainsi, est mis en place un régime intermédiaire entre le système de l'autorisation réclamé par les premières législations de protection des données ou par certaines législations à propos de fichiers particuliers (cf. à ce propos l'article 18, al. 5, du projet de directive) et un système de liberté complète où la Commission n'interviendrait qu'a posteriori, c'est-à-dire en cas de litige. Un tel système s'il a l'avantage d'instaurer une certaine transparence pour l'autorité de contrôle est cependant considéré par certains, y compris la Commission belge, et ce au vu des expériences étrangères, comme un système administratif lourd voire inutile à partir du moment où l'existence obligatoire d'un registre permet à cette autorité de prendre connaissance des données essentielles du système d'information du ficheur.

Rejeté dans un premier temps par le premier projet de directive, le système de déclaration a cependant été repris dans la seconde version actuellement en discussion (article 18 et s.).

36. La déclaration moyennant versement d'une contribution consiste en une fiche d'identification du traitement : elle reprend :

1° la date de la déclaration et, le cas échéant, la mention de loi, du décret, de l'ordonnance ou de l'acte réglementaire décidant la création du traitement automatisé;

2° les nom, prénoms et adresse complète ou la dénomination et le siège du maître du fichier et, le cas échéant, de son représentant en Belgique;

3° les nom, prénoms et adresse complète ou la dénomination et le siège du gestionnaire du traitement automatisé;

4° la dénomination du traitement automatisé;

5° le but poursuivi par le traitement automatisé;

6° les catégories de données à caractère personnel qui sont traitées avec une description particulière des données visées aux articles 6 à 8;

7° les catégories de personnes admises à obtenir les données;

8° les garanties dont doit être entourée la communication des données aux personnes visées au 7°;

9° les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit;

10° la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées.

La loi autorise le cas échéant (art. 17, § 4, de la loi) la Commission à demander d'autres éléments d'informations comme "l'origine des données, la technique d'automatisation choisie et les

mesures de sécurité prévues". Les flux transfrontières même occasionnels obligent le ficheur à des mentions supplémentaires sur les catégories de données exploitées et leur pays de destination. Chaque modification ou suppression d'un élément de la déclaration donnent lieu à une nouvelle procédure de déclaration (art. 17, § 7). Le non respect de l'obligation de déclaration est assorti d'une sanction pénale (amende) selon l'article 39, 7°, de la loi.

37. Il est trop tôt pour apprécier la manière dont la Commission interprétera les diverses mentions à déclarer et fixera les modalités pratiques de cette déclaration. Ainsi quel degré de précision exigera-t-elle dans la description du but (finalité ?) poursuivi par le traitement automatisé? Même question à propos des catégories de personnes admises à obtenir les données et des garanties dont est entourée la communication à ces personnes ? Il est clair qu'une interprétation trop laxiste rendrait inutile la déclaration mais qu'à l'inverse, un excès de précision sera ressenti comme une charge intolérable pour les entreprises. La mention obligatoire de la durée de la conservation des données contraste avec l'absence de tout principe général limitant la durée du traitement aux nécessités déduites de la finalité du traitement (cf. supra n° 23). L'exemple étranger et le projet de directive invitent à mieux distinguer les catégories d'utilisateurs internes, d'une part, et les tiers à qui communication est faite, d'autre part.

Outre ces réflexions sur le contenu de la déclaration, deux remarques relatives à l'extension de l'obligation doivent encore être énoncées :

— la loi belge reprend le système français de déclaration simplifiée voire d'exemption de déclaration pour les catégories de traitement ne présentant manifestement pas de risques d'atteinte à la vie privée (art. 17, § 8) mais l'entrevoit comme un régime décidé par arrêté royal et non par la seule Commission, ce qui, refrain connu (voir supra n° 30), ôte à ce système une certaine souplesse, risque de mettre la Commission hors jeu mais -c'est son seul mérite- la maintient dans un rôle de pur conseil et non de décideur;

— la loi belge prévoit que la déclaration peut également être exigée de certains fichiers manuels : la Commission en décide seule cette fois (art. 19).

Enfin, on ajoutera que si la déclaration doit ouvrir à la Commission la possibilité d'un examen complémentaire relatif à la légitimité et à la conformité d'un traitement c'est dans un délai de trois jours (quinze selon le projet de directive) qu'elle doit adresser l'accusé de réception qui, n'équivaudra en aucune manière, on le conçoit à un jugement du bien fondé de l'activité du ficheur.

§ 3. La transparence externe : le registre public créé par l'article 18

38. Un fichier des fichiers, reprenant les mentions de la déclaration est institué par la loi auprès de la Commission. Il est accessible au public et l'inscription d'un traitement à ce registre fait l'objet de l'octroi

d'un numéro d'identification qui "devra figurer sur toute pièce qui en matérialisera l'usage".

L'idée d'un numéro d'identification est originale : le numéro devant figurer sur toute correspondance du ficheur avec le fiché, il permettrait à ce dernier, par exemple en cas de réception d'un mailing non désiré, de retrouver aisément le maître du fichier.

§ 4. La transparence vis-à-vis du fiché lors de la collecte de renseignements auprès de lui

39. L'article 4 prévoit que lors de la collecte des données nominatives auprès de la personne concernée, le ficheur informe ce dernier de l'identité du maître du fichier, de la finalité de la collecte et, le cas échéant, de sa base légale ou réglementaire, de l'existence du registre public et du droit d'accès. Les modalités de mise à disposition de cette information ne sont pas définies : sans doute, faudra-t-il raisonner ici comme en matière de conditions générales contractuelles et autoriser, par exemple, qu'un commerçant remplisse son obligation par une affiche apposée à un endroit ad hoc.

Ceci dit, on s'étonnera du peu d'informations à transmettre par le ficheur. L'article 11 du projet de directive ajoute à la liste belge, les informations suivantes : le caractère obligatoire ou non de la réponse, les conséquences d'un défaut de réponse, le destinataire ou les catégories de destinataires des données. A cette première lacune de la loi belge s'ajoute l'absence d'un principe général relatif aux modes de collecte. Tant la convention du Conseil de l'Europe que le projet de directive affirment hautement le principe suivant lequel les modes de collecte doivent être licites et loyaux, que la collecte ait lieu auprès de la personne concernée ou auprès de tiers. Ainsi, les autorités de protection des pays qui nous entourent ont elles exigés que la surveillance des employés par caméra vidéo, les enregistrements automatiques des appels pratiqués par ces derniers et la localisation à distance des employés circulant pour le compte de la firme fassent l'objet de procédures claires d'information de la part de la firme à l'intention de ses employés.

II. L'obligation de sécurité

40. Par obligation de sécurité, il faut envisager au sens de l'article 16, non les seules mesures techniques dont peut être entourée la mise en œuvre des traitements mais toute mesure technique ou organisationnelle destinée à assurer le respect effectif des dispositions légales. Ainsi l'article 16, § 2, oblige le maître du fichier à informer les utilisateurs internes des données des prescrits de la loi et des exigences découlant de l'application du principe de finalité. Cette disposition conduira vraisemblablement les entreprises d'une certaine taille à nommer un responsable interne, préposé à veiller au respect et à la mise en œuvre des prescrits légaux et à rendre conscient chaque membre de l'entreprise des conséquences de la législation. Peut-être, eût-il été bon, suivant l'exemple allemand, d'obliger les entreprises et administrations à nommer une personne physique responsable interne de la protection des données.

41. Au-delà de ce premier point, l'obligation de sécurité exige (article 16 § 2) la vérification de la conformité des programmes servant au traitement automatisé avec les termes de la déclaration) et la prise de mesures afin de réserver l'accès aux seules personnes autorisées sur base des finalités et d'interdire les modifications, ajouts, effacements, lectures et rapprochements ou interconnexions non autorisés.

"Le maître du fichier doit enfin adopter (article 16 § 3) les mesures techniques et organisationnelles adéquates en vue de garantir la sécurité des données. L'exigence de sécurité technique doit être comprise comme un moyen contribuant à assurer la protection de l'individu contre les tiers qui ne seraient pas autorisés à accéder aux données et à les utiliser. Plus exactement, le maître du fichier est tenu de "protéger les fichiers contre la destruction accidentelle ou non autorisée, contre la perte accidentelle, ainsi que la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel".

Le degré de protection doit être adéquat eu égard, d'une part, à l'état de l'art en la matière et aux dépenses suscitées par les mesures adoptées, d'autre part, aux menaces virtuelles et à la nature des données à prémunir. On peut s'interroger sur l'interprétation à donner à la notion de "dépenses suscitées". Faudra-t-il l'évaluer au regard des moyens du maître du fichier ? Si l'on retient ce critère, la sécurité des données pourrait être plus ou moins bien assurée en fonction de la capacité financière du maître du fichier.

En ce qui concerne les obligations relatives à la gestion, l'exposé des motifs précise qu'il ne s'agit que d'obligations de moyen, dont l'appréciation devra donc être raisonnable. Ainsi, seront considérées comme nécessaires les mesures "dont l'effet de protection est dans un rapport adéquat avec les efforts qu'elles occasionnent" (BOULANGER-de TERWANGNE-LEONARD).

Conclusions

42. Les législations de protection des données appellent les ficheurs à s'interroger sur les raisons et les limites de leur droit à l'information. En ce sens, elles en appellent d'abord à la responsabilité propre de l'entreprise, c'est à elle que revient la tâche de définir les finalités de ses traitements, d'en apprécier la légitimité et à partir de là d'en circonscrire le contenu pertinent et les utilisateurs. Au-delà, les entreprises se devront de rendre transparents leurs choix et, concrètement, de prévoir les mesures organisationnelles et techniques, propres à assurer le respect de la loi.

43. La loi belge correspond à ce paradigme. Sans doute, se plaindra-t-on de distinctions insuffisantes entre ficheurs, de l'affirmation incomplète du principe de finalité, de l'absence de réglementation des communications; sans doute, soulignera-t-on le manque de souplesse dans l'appréciation de la conformité, souplesse qu'aurait permis l'introduction de la notion de "consentement" ! Peut-être estimera-t-on que la transparence ait pu être mieux assurée et regrettera-t-on que la créa-

tion d'un "homme relais", chargé au sein des entreprises du respect des prescrits légaux, n'ait pas été évoquée. Mais au-delà de ces imperfections, la législation a le mérite d'exister et de donner à la Commission et au juge les instruments d'un contrôle au service de libertés contradictoires qu'ils auront pour charge d'arbitrer dans un contexte technologique, social et culturel toujours changeant.

BIBLIOGRAPHIE SOMMAIRE

BERLEUR, J., et POULLET, Y., Le droit à la vie privée selon le projet Gol, J.T., 1982.

BOULANGER, M.H., et de TERWANGNE, C., Commentaire de la proposition de directive du Conseil relative à la protection des personnes à l'égard du traitement des données à caractère personnel, Cahiers Lamy Droit de l'informatique, n° 40, 1992.

BOULANGER, M.H. et de TERWANGNE, C., LEONARD, Th., La loi du 8 décembre 1992, J.T., 1993 (à paraître).

DEJEMEPPE, P., La mémoire de l'argent. La protection des données à caractère personnel dans la loi du 12 juin 1991 relative au crédit à la consommation, D.C.C.R., janvier 1992, n° 14.

FRAYSSINET, J., Informatique, fichiers et libertés - Les règles, les sanctions, la doctrine de la C.N.I.L., Paris, Litec, 1992.

LEONARD, Th., et POULLET, Y., Les libertés comme fondement de la protection des données nominatives, in F. RIGAUX, "La vie privée une liberté parmi les autres ?", Travaux de la Faculté de Droit de Namur n° 17, Bruxelles, Larcier, 1993.

MEYSMANS, E., Bancaire bestanden en privacy-bescherming in België, Computerrecht, 1992, n° 1.

MEYSMANS, E., De wet tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens : gevolgen voor de bank-sector, in Vie privée, Journée d'information, Bruxelles, 18 mars 1993, A.B.B.

POULLET, P. et Y., Applicabilité aux entreprises d'une législation protectrice des données, in Banques de données, entreprises, vie privée, actes du colloque tenu à Namur les 25 et 26 septembre 1980, Bruxelles, CIEAU-CREADIF.

RIGAUX, F., La protection de la vie privée à l'égard des données à caractère personnel, Annales de droit de Louvain, 1993/1.

ROBBEN, F., Recente ontwikkelingen m.b.t. het Belgische wetsontwerp tot bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens, Computerrecht, 1992, n° 5.

SIMITIS, S., Initiatives taken by the european Communities in the field of data protection : What will change ?, XIIIème Conférence des Commissaires à la protection des données, 2-4 octobre 1991, Conseil de l'Europe, Strasbourg, 1992.

Textes législatifs :

- Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Série des Traités européens, janvier 1981; n° 108, elle est entrée en vigueur le 1er octobre 1985, signée par la Belgique en 1982.

- Proposition modifiée de directive du Conseil 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, J.O.C.E., n° C 311 du 27 novembre 1992, p. 30 et ss.

- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, M.B., 18.03.1993.

L'EXPERIENCE FRANÇAISE

par Mme Louise CADOUX,
Vice-Président délégué
de la Commission Nationale de l'Informatique
et des Libertés (France).

Je n'ai ni la notoriété ni le talent de Monsieur FAUVET, Président de la Commission française Nationale de l'Informatique et des Libertés mais, étant tombé malade hier, il m'a demandé de le suppléer. Je tâcherai de le faire du mieux que je pourrai, en suivant les quelques notes qu'il a bien voulu me confier hier soir pour que je puisse organiser l'exposé.

Monsieur FAUVET, au sujet duquel vous devez savoir qu'il était journaliste à l'origine, a souhaité dès le début de cette intervention que soient mis en vedette trois textes et trois articles. En effet, il a voulu que nous rappelions ici, à l'occasion de la mise en place de la Commission belge, quel était l'objectif poursuivi et il a voulu indiquer quels étaient les rapports de subordination de l'informatique par rapport à un certain nombre de valeurs auxquelles nous croyons tous dans le monde occidental.

* * *

Ces trois textes, qu'il a voulu mettre en vedette, pour des motifs presque philosophiques, sont, honneur oblige, la loi française du 6 janvier 1978 dont l'article 1er dit ceci : "*L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*"

Ce premier texte est un texte de principe, ce qui est rare, dans notre droit interne français. En effet, de pareilles déclarations de principe figurent, en général, dans des exposés des motifs et non dans les parties normatives des textes. Mais le fait que le législateur de 1978 ait voulu déroger à cette règle en inscrivant ce principe dans l'article 1er de la loi française, est l'indication qu'il voulait que l'informatique soit subordonnée à ces valeurs fondamentales.