La protection de la vie privée à l'égard des traitements de données à caractère personnel

Léonard, Thierry; De Terwangne , Cécile

Published in:
Journal des Tribunaux

Publication date:
1993

Document Version
le PDF de l'éditeur

Journal des tribunaux

15 mai 1993
112e année - N° 5675

Bureau de dépôt : Bruxelles X
Hebdomadaire, sauf juillet/août

Editeurs : Maison LARCIER, s.a., rue des Minimes, 39 - 1000 BRUXELLES
Edmond Picard (1881-1899) - Léon Hennebicq (1900-1940) - Charles Van Reepinghen (1944-1966) - Jean Dal (1966-1981)

ISSN 0021-812X

LA PROTECTION DE LA VIE PRIVEE A L'EGARD DES TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

La loi du 8 décembre 1992

PLAN

SOMMAIRE

PRIX DU
Journal des tribunaux
(1993)

REGLEMENT

Article 1er. — Le « Journal des tribunaux » organise chaque année un concours ayant pour objet de couronner la meilleure note sous décision.

L'épreuve est ouverte, pour 1993, à tous les licenciés en droit qui ont obtenu leur diplôme après le 1er janvier 1990.

Les candidats ne peuvent participer qu'une seule fois à ce concours.

Article 2. — L'auteur de la note jugée la meilleure se voit normalement décerner le « Prix du Journal des tribunaux », qui comporte : - l'attribution d'une somme de 15.000 F; - le service gratuit du journal pendant un an; - le service gratuit pendant un an des « Dossiers du Journal des tribunaux » et du « Larcier cassation », publiés sous le patronage du *Journal des tribunaux*.

La note couronnée est publiée.

Article 3. — C'est une décision relative au droit des personnes qui sera soumise cette année à la sagacité et à l'érudition des candidats.

Article 4. — La demande d'inscription au concours doit parvenir au rédacteur en chef, chaussée de La Hulpe, 187, 1170 Bruxelles, avant le 15 juin 1993. Elle indiquera les nom, prénoms, profession et adresse du candidat, ainsi que la date de son diplôme.

Article 5. — Les candidats doivent adresser leur note au rédacteur en chef, avec le texte de cette décision précédé de l'argument et du sommaire proposés, pour le 31 août 1993 au plus tard.

INTRODUCTION

1. — En adoptant, dans un rare élan d'unanimité, la loi sur la protection de la vie privée à l'égard des traitements de données à caractère personnel (1), la classe politique entend répondre à un problème de société. Un large consensus s'est formé sur la nécessité de préserver l'individu d'une mise en fiches anarchique qui reviendrait à une mise en pièces de sa vie privée. L'idée d'une telle loi fait son chemin depuis plus de vingt ans (2). Les développements constants de l'informatique ont progressivement permis le traitement automatisé systématique des données à caractère personnel. De ce fait, le risque d'utilisation et de diffusion abusive de l'information emmagasinée n'a cessé de s'accroître. Une intervention législative s'imposait.

L'informatique n'a pas du jour au lendemain investi le champ de la vie privée pour dérober aux individus des données à caractère personnel qu'ils entendaient cacher. Les données traitées par l'informatique ne sont généralement pas secrètes; la plupart étaient souvent même déjà traitées dans des fichiers manuels. La technique informatique n'est qu'un moyen d'information qui raccourcit les espaces et élargit les horizons. Le village planétaire que contribuerait à créer l'informatique ne s'apparente toutefois que de très loin au village campagnard d'antan. Au sein de ce dernier, l'individu conserve la maîtrise de son image véhiculée. Il finira toujours par savoir ce qui se dit à propos de sa personne, qui fait circuler les bruits et à quelle fin l'information est diffusée. Au besoin, il pourra rectifier les erreurs et prévenir les abus. Il en va autrement dans le village planétaire, « McMonde » (3) dans lequel l'individu perd la maîtrise de son image informationnelle (4). Les informations circulent en dehors de tout contrôle de la part des individus qu'elles concernent. Rien n'empêche dès lors un usage abusif (sélectif et discriminatoire, par exemple) des données personnelles. Sans nier l'utilité de la circulation de l'information, il faut constater qu'en l'absence de garde-fous juridiques une information semée à tout vent appauvrit la personnalité des individus. Le « McMonde » finit en effet par réduire cette personnalité à quelques données à caractère personnel : à la rencontre individuelle se substitue une série de mises en profil à distance sur des bases objectives, certes, mais totalement désincarnées.

La loi sur la protection de la vie privée à l'égard des traitements de données à caractère personnel se place à contre-courant de cette dérive induite du progrès technologique. Elle vise précisément à protéger ce pan de plus en plus menacé de la vie privée des individus : leur image informationnelle. L'objectif du législateur est de restituer à l'individu la maîtrise de cette image. S'il n'est pas toujours en droit de décider souverainement des informations qui peuvent circuler sur son compte, il peut les contrôler et en vérifier l'usage. La loi vient à point nommé, non seulement pour concrétiser deux décennies de réflexion législative continuellement remise en cause par les progrès de l'informatique, mais aussi pour affirmer de façon générale le principe de la protection de la vie privée des individus vis-à-vis des traitements de données à caractère personnel. Ce faisant, la loi comble partiellement une lacune du droit belge où aucun texte spécifique ne protège la vie privée, si ce n'est l'article 8 de la Convention européenne des droits de l'homme. Elle actualise aussi l'engagement pris par la Belgique en 1982 à l'égard des pays cosignataires de la Convention n° 108 du Conseil de l'Europe. Ce texte enjoignait aux parties d'adopter une législation interne réglementant la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (5). Destinée pour partie à apurer une dette du passé, la nouvelle loi pourrait également produire des dividendes pour l'avenir. En effet, une proposition de directive européenne sur le même sujet s'élabore progressivement (6). Mis au courant des intentions de la Commission des Communautés européennes, le législateur a veillé à anticiper l'obligation qui ne manquera pas de lui être imposée par le législateur européen.

2. — A la recherche d'un équilibre entre la nécessité d'une circulation de l'information et la conservation des droits individuels, la nouvelle loi subordonne les traitements de données à caractère personnel au respect de plusieurs principes et modalités en réglementant les relations entre les « ficheurs » et les « fichés ». Cette démarche est classique dans le paysage normatif européen.

Le fondement de l'intervention législative trouve son expression dans le principe de protection de la vie privée énoncé à l'article 2. Celui-ci pose en termes clairs que toute personne physique a *droit au respect de sa vie privée* lors du traitement de données à caractère personnel qui la concernent.

Ce droit n'est toutefois pas reconnu de manière absolue. Le consacrer de la sorte conduirait à paralyser l'activité administrative, économique et sociale. Le souci de ménager l'intérêt de la société à l'information et celui de l'individu à voir sa vie privée protégée a incité le législateur à affirmer un deuxième principe fondamental : le *principe de finalité*. Selon celui-ci, tout traitement de données à caractère personnel doit poursuivre un but légitime. C'est dans l'évaluation de la légitimité que se situera la recherche de l'équilibre entre les deux intérêts contradictoires en présence. Le principe de finalité implique en outre que le traitement soit opéré dans un but déclaré. Il ne sera plus question désormais de mettre en œuvre des traitements occultes.

Pour être admises, les opérations doivent respecter la finalité annoncée. On peut dès lors enregistrer des données, les communiquer à des tiers ou les conserver, pour autant que ces opérations se justifient au regard du but légitime déclaré. Toutefois, certaines données sont soumises à un régime plus restrictif en raison du danger de discrimination propre à leur nature (données « sensibles »).

Sans être énoncé en termes exprès, un *principe de transparence* des circuits d'information à l'égard de l'individu sous-tend l'ensemble du texte. Il s'exprime dans diverses obligations. Ainsi, toute personne fichée doit être informée de l'existence d'un traitement portant sur les données qui la concernent; tout traitement automatisé doit faire l'objet d'une déclaration dont les mentions principales sont consignées dans un registre accessible au public.

La mise en œuvre de ces principes implique que des droits soient reconnus à la personne concernée par les données et que des obligations soient corollairement mises à charge de celui qui traite celles-ci. L'individu fiché aura de la sorte le droit d'accéder aux données le concernant et de les faire rectifier si nécessaire. Le responsable du traitement, pour sa part, doit garantir l'exercice effectif de tels droits; d'autres obligations pèsent également sur lui, notamment veiller à ce que les données soient exactes et mises à jour.

Le contrôle du respect du régime de protection mis en place par la loi est réparti entre différents acteurs. Un premier contrôle s'effectue lorsque l'individu exerce ses droits d'accès et de rectification. La loi institue par ailleurs, une Commission administrative, la Commission de protection de la vie privée, dont la mission spécifique est de veiller à l'application de la réglementation. Enfin, les cours et tribunaux restent compétents pour connaître de toute violation des prescriptions légales.

Cette étude analyse dans un premier temps le champ d'application de la loi - ce qui passe nécessairement par une définition des concepts clefs - [1] avant de décrire et commenter les lignes directrices de la protection mise en place [2] et les nouveaux droits et obligations instaurés par le législateur [3]. L'examen du statut et du rôle de la Commission de contrôle instituée comme gardienne de l'équilibre consacré par la loi [4], des sanctions pénales destinées à punir les violations de cet équilibre et des modalités d'entrée en vigueur de la loi [5], complète la réflexion.

(1) Loi du 8 décembre 1992, *M.B.*, 18 mars 1993, pp. 5801 et s.

(2) La première proposition de loi remonte à 1971 : proposition de loi relative à la protection de la vie privée et de la personnalité, *Doc. parl.*, Sén., sess. 1970-1971, n° 706; de nombreux projets de textes firent suite, notamment : projet de loi relatif à la protection de certains aspects de la vie privée, *Doc. parl.*, Sén., 1975-1976, n° 846/1 et projet de loi relatif à la protection de la vie privée à l'égard des traitements automatisés de données à caractère personnel (« projet Gol »), *Doc. parl.*, Ch. repr., sess. 1984-1985, n° 1330/1; sur ce dernier projet J. Berleur et Y. Poullet, « Le droit à la vie privée selon le projet Gol », *J.T.*, 1982, p. 769.

(3) Selon l'expression du professeur B. Barber (*Libération*, 4 janv. 1993).

(4) C'est la Cour constitutionnelle allemande qui la première, dans un arrêt du 15 décembre 1983, utilisa l'expression « droit à l'autodétermination informationnelle » (ou maîtrise de son image informationnelle) dans un raisonnement basé sur la protection constitutionnelle du droit à l'épanouissement de la personnalité (*Recht auf informationelle Selbstbestimmung*, BVerfGE 65, 1).

(5) Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, *Série des Traités européens*, signée par la Belgique en 1982, elle est entrée en vigueur le 1er octobre 1985.

(6) 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, 27 nov. 1992, pp. 30 et s.

1. — LES DEFINITIONS ET LE CHAMP D'APPLICATION DE LA LOI

3. — La portée de la protection mise en place par la loi du 8 décembre 1992 se déduit de l'analyse des concepts techniques définis à l'article 1er de la loi.

Les notions de « données à caractère personnel », d'une part, de « traitements » et « fichiers », d'autre part, permettent de cerner l'objet de la protection. Les concepts de « maître du fichier » et de « gestionnaire du traitement » concourent à identifier un responsable, garant de la protection accordée et interlocuteur privilégié des personnes protégées.

1.1. — Les définitions

1.1.1. — *Les données à caractère personnel*

4. — Aux termes de l'article 1er, § 5, les données « réputées 'à caractère personnel' » sont celles « relatives à une personne physique identifiée ou identifiable ». Cette définition appelle deux commentaires.

5. — La loi ne précise pas ce qu'il faut entendre par « donnée » (7). Il reviendra à la Commission de la vie privée et le cas échéant, au juge, d'interpréter cette notion. Toutefois, les travaux préparatoires laissent déjà entendre qu'une « donnée » ne vise pas seulement une information écrite ou chiffrée mais aussi l'information contenue dans une image, une bande son, ou une empreinte digitale (8).

Les spécificités de la donnée sont sans conséquence au regard de la loi. Comme le notait un auteur relativement à la législation française, « peu importe si l'information est sensible ou non, protégée ou facilement accessible; peu importe son sens et son objet (...) » (9).

6. — Toute donnée ne rentre pas forcément dans le champ d'application de la loi. Elle doit permettre d'identifier une personne physique. Les personnes morales et les groupements sont donc exclus de la protection légale et ce, à juste titre, selon nous, sous peine de sortir du champ strict de la vie privée. Bien entendu si les données relatives à des personnes physiques (les noms des administrateurs d'une société, ou des membres d'une association sans but lucratif) sont intégrées parmi des informations portant sur des personnes morales ou autres groupements, elles bénéficient de l'ensemble de la protection accordée par la loi (10).

Le texte ne précise pas à partir de quand une donnée porte sur une personne identifiable (11). Le plus souvent, le caractère personnel des données apparaît directement. C'est le cas par exemple de traitements centralisant des renseignements sur l'état de santé d'individus dont le nom est conservé en regard d'autres données (maladies contractées, dates d'interventions chirurgicales, etc.). Il arrive que le caractère personnel des données ressorte indirectement. Ainsi, lorsque certaines données relatives à un individu sont reprises sous un numéro d'identification ou lorsqu'une étude statistique produit des résultats à ce point précis qu'elle permet, sans efforts excessifs, de retrouver les personnes concernées (12).

1.1.2. — *Le traitement automatisé et la tenue de fichiers manuels*

7. — L'émergence de lois de protection de la vie privée à l'égard des traitements de données s'explique par la crainte des législateurs face à l'informatisation croissante de la société. L'évolution rapide de l'outil interdit d'envisager une législation qui viserait une technique particulière d'utilisation des données. Légiférer en fonction de techniques spécifiques aboutirait à un texte rapidement dépassé. Avec sagesse le législateur a opté pour des concepts abstraits, instaurant « un cadre dans lequel la technique pourra évoluer » (13). Par là, l'accent est mis sur la véritable origine des menaces d'atteinte à la vie privée de l'individu. Ce dernier n'est pas protégé contre une technique précise mais bien contre les usages multiples qu'autrui pourrait faire à partir des données.

Se dégageant d'une approche basée sur l'outil, le législateur fonde la protection sur le concept de traitement, c'est-à-dire d'opérations effectuées sur les données. Il importe peu que l'enregistrement de l'identité d'une personne, de son adresse et de son numéro de compte se fasse par stockage sur une disquette, sur une bande ou une carte magnétique, dans un cahier papier, etc. Seules les diverses tâches que ces instruments remplissent sont prises en considération par la loi (14).

8. — Au sens de l'article 1er, § 1er, le traitement couvre tant « le traitement automatisé » que « la tenue d'un fichier manuel ». A la notion de traitement automatisé est donc censée répondre celle de tenue d'un fichier manuel. Cette conception révèle une confusion; on oppose sous le terme générique de traitement deux notions radicalement différentes. Si elles représentaient

(7) Contrairement à d'autres textes; voy. Convention n° 108 du Conseil de l'Europe qui vise en son article 2.a « toute information »; la loi française (L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.*, 7 et rectif. 25 janv. 1978) parle quant à elle d'« informations (...) sous quelque forme que ce soit » (art. 4).

(8) Dans le même sens voy. la déclaration d'un membre de la Commission de la vie privée (*in* Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445-2, p. 19) ainsi que la réponse du ministre (*idem*, p. 57); voy. aussi pour information l'article 1er, alinéa 2, du projet de loi québécois (Projet de loi 68 - Loi sur la protection des renseignements personnels dans le secteur privé, *Assemblée nationale - seconde session - trente-quatrième législature*, éditeur officiel du Québec, 1992) qui déclare que la loi « s'applique à ces renseignements (...) quelle que soit la forme sous laquelle ils sont accessibles : écrite, graphique, sonore, visuelle, infomatisée ou autre ».

(9) J. Frayssinet, *Informatique, fichiers et libertés - Les règles, les sanctions, la doctrine de la C.N.I.L.*, Paris, Litec, 1992, p. 35, n° 82.

(10) Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel - Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 1990-1991, n° 1610/1, p. 6; voy. pour un exemple d'application en France la délibération de la C.N.I.L. n° 82-69 du 4 mai 1982 (C.N.I.L., *Troisième rapport d'activité - 15 octobre 1981- 15 octobre 1982*, Paris, La Documentation française, 1983, pp. 30 et s.) relative au fichier bancaire des entreprises (FIBEN) de la Banque de France qui centralise un ensemble de renseignements relatifs à l'activité économique des entreprises et de leurs dirigeants (sur ce fichier voy. aussi C.N.I.L., *Huitième rapport d'activités-1987*, Paris, La documentation française, 1988, pp. 160 à 162); certains auteurs français vont même plus loin en considérant que des informations relatives à des entreprises mais étroitement liées à leurs dirigeants tombent dans le champ d'application de la loi. Dans le prolongement de cette idée, un traitement relatif aux entreprises unipersonnelles à responsabilité limitée devrait être considérée comme relevant de la loi (M. Guibal, Ch. Le Stanc, L. Rapp, M. Vivant, *Lamy - Droit de l'informatique - Informatique, télématique, réseaux*, Lamy, Paris, 1992, n° 1152); voy. aussi J. Frayssinet, *op. cit.*, p. 36, n° 86 et réf. cit.

(11) Contrairement à la loi, la proposition de directive européenne indique en son article 2. a : « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Ne sont pas considérées comme à caractère personnel les données agrégées sous forme statistique, de telle sorte que les personnes concernées ne sont plus raisonnablement identifiables ».

(12) Voy. pour un exemple le cas de recensement de populations par îlots et les solutions préconisées par la C.N.I.L. afin d'éviter la violation de la règle de l'anonymat, C.N.I.L., *Onzième rapport d'activités-1990*, Paris, la Documentation française, 1991, pp. 161 et s.; pour un relevé fouillé des cas retenus en France comme informations nominatives (l'équivalent des données à caractère personnel en Belgique) voy. M. Guibal, Ch. Le Stanc, L. Rapp, M. Vivant, *op. cit.*, n° 1152.

(13) Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445/2, p. 19; voy. aussi J. Frayssinet, *op. cit.*, p. 36, nos 87 et s.

(14) C'est donc à tort, selon nous, que le ministre de la Justice lors des débats parlementaires déclare que « lorsque l'on dénomme un traitement, cela signifie que l'enregistrement et la modification des données sont réalisés sur telle machine et selon tel programme » (Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch., sess. extr. 1991-1992, n° 413/12, p. 15). Une telle conception ne permettrait pas de rendre compte de la tendance à l'intégration des traitements informatisés. Alors qu'auparavant le système consistait en une multitude de « fichiers » cloisonnés qui contenaient toutes les données nécessaires aux traitements dont elles faisaient l'objet, il a maintenant la capacité de ne retenir qu'une fois les données dans sa mémoire et de les rechercher chaque fois qu'une utilisation spécifique de celles-ci est nécessaire (Pour une réflexion analogue concernant cette fois les fichiers bancaires voy. E. Meysmans, « Bancaire bestanden en privacy-bescherming in België », *Computerrecht*, 1992, n° 1, p. 10). Le traitement se fait par l'intermédiaire d'importantes bases de données représentant à elles-seules une entité physique unique rencontrant de multiples finalités distinctes. Ces bases de données s'intègrent également de manière plus large dans le système informatique utilisé. Dès lors, les traitements sont effectuées par le biais de nombreux ordinateurs reliés entre eux et fonctionnant grâce à une grande diversité de logiciels. A l'unité de l'outil répond l'éclatement des tâches sans cependant qu'il y ait création de nouvelles mémoires. On est déjà très loin de la conception du ministre...

deux facettes d'une réalité unique, ces deux notions devraient forcément présenter certaines analogies. Tel n'est pas le cas puisque l'une, le fichier (15), vise un ensemble de données et l'autre, le traitement, des opérations qui leur sont appliquées.

1.1.2.1. — *Le traitement automatisé.*

9. — L'article 1er, § 3, de la loi définit le traitement automatisé comme « tout ensemble d'opérations réalisées en tout ou en partie à l'aide de procédés automatisés et relatif à l'enregistrement et la conservation de données à caractère personnel, ainsi qu'à la modification, l'effacement, la consultation ou la diffusion de ces données ».

Pour qu'il y ait traitement automatisé, trois conditions doivent donc être remplies :

— Il faut d'abord que des opérations soient effectuées sur les données. Le texte en prévoit six types : l'enregistrement, la conservation, la modification, l'effacement, la consultation et la diffusion. Ces termes généraux ont vocation à être largement interprétés. Ainsi, ce n'est pas parce que la communication n'est pas comme telle reprise dans la liste qu'elle ne représente pas une opération susceptible de faire partie d'un traitement; il s'agit en fait d'une diffusion (16) particulière de données (17).

— Il faut ensuite que les opérations soient effectuées en tout ou en partie à l'aide de procédés automatisés. La notion de procédé automatisé est extrêmement vague ce qui permet d'englober à peu près toutes les nouvelles technologies de l'information (informatique, télématique, réseaux de télécommunication, etc.). Sont seuls exclus de la définition les systèmes de traitement qui font appel exclusivement à des procédés manuels (par exemple, un fichier papier classant nominalement les membres du personnel d'une p.m.e., chaque fiche contenant des informations du type âge, état civil, poste, rémunération, etc.). Remarquons qu'il est nécessaire, mais suffisant, qu'à un moment de la procédure de traitement de l'information intervienne un procédé automatisé pour que l'ensemble des opérations constitue un traitement automatisé au sens de la loi. Ainsi, dans l'exemple précité, si les fiches papiers sont classées suivant des numéros d'identification repris ensuite dans la mémoire d'un ordinateur — ce qui facilite la recherche des fiches — l'ensemble du traitement sera réputé automatisé.

— Il faut encore que ces opérations forment un ensemble. A notre sens, le critère unificateur réside dans la finalité « générique » poursuivie par le traitement. A chaque traitement correspond un certain nombre d'opérations participant toutes à la réalisation d'un même but. Ainsi, une entreprise effectue une série d'opérations sur les données de son personnel en vue du paiement de leur rémunération; l'enregistrement des données, mais aussi leur rapprochement (par exemple le rassemblement de toutes les sommes versées à un individu durant une période déterminée), voire leur diffusion limitée (envoi des fiches de salaires, envoi de données aux organismes de sécurités sociales), constituent des applications poursuivies en vue de la réalisation d'une seule et même finalité, le payement du personnel. Par conséquent, la finalité est également le critère de distinction des traitements entre eux.

10. — Ces traitements automatisés correspondent, dans la réalité, à un nombre impressionnant d'applications différentes. Outre les cas classiques de la mise en mémoire informatique et l'utilisation de données à caractère personnel en vue de la bonne gestion d'une activité ou d'une mission spécifique (« traitements » clients, de population, de marketing, de personnel, etc.), certaines manipulations de données sont susceptibles d'être visées par la loi sans que cela n'apparaisse avec autant d'évidence. Ainsi en est-il notamment des traitements consistant dans : l'utilisation de badges électroniques permettant de contrôler les déplacements de personnes dans une entreprise (ou une administration), l'utilisation d'une carte à mémoire, une procédure automatisée de recrutement de personnel (questionnaires à choix multiples dont les réponses sont « lues » par un logiciel particulier), toute forme de marketing fonctionnant sur le ciblage des destinataires, les systèmes automatisés de prospection téléphonique, la mise en place et l'utilisation de systèmes experts, les systèmes vidéo de surveillance (18), etc. (19).

1.1.2.2. — *La tenue d'un fichier manuel.*

11. — Avant de décrire ce que vise la loi par « tenue d'un fichier manuel », il convient de préciser ce qu'il faut entendre par la notion de « fichier ».

12. — L'article 1er, § 2, définit le fichier comme « un ensemble de données à caractère personnel, constitué et conservé suivant une structure logique devant permettre une consultation systématique ».

Au sens le plus classique du terme, le fichier désigne un simple ensemble de données traitées en vue d'une utilisation particulière. En subordonnant l'existence du fichier à une condition particulière de structuration, la loi participe à une tendance risquant de se généraliser au sein des législations « privacy » européennes (20), visant à exclure les dossiers de leur champ d'application.

Le critère de distinction entre dossier et fichier repose sur le degré de structuration de l'information (21). A la différence du dossier, le fichier *permet une consultation systématique des données qu'il contient*. La portée de cette expression est particulièrement vague. Comme le rappelle la Commission de la vie privée « connaissons-nous un seul dossier qui n'a pas pour fin d'être consulté ? A quoi servirait-il s'il ne contenait pas d'informations susceptibles de l'être ? Le propre d'un dossier est justement de regrouper un certain nombre de données sur un sujet délimité afin d'éviter une dissémination de celles-ci » (22). C'est donc précisément sur le caractère systématique de la consultation que semble se fonder la distinction fichier-dossier. Etablir ce caractère risque de donner lieu à un travail délicat d'interprétation et de générer une insécurité juridique préjudiciable.

(15) Cette notion semble d'ailleurs tomber de plus en plus en désuétude. Sur ce point, voy. S. Simitis, « Initiatives taken by the European Communities in the field of data protection : What will change ? », *Treizième conférence des Commissaires à la protection des données* (2-4 octobre 1991), Conseil de l'Europe, Strasbourg, 1992, p. 61). On retrouve encore ici l'idée selon laquelle le danger pour l'individu provient moins des données (cf. le fichier) que de leur utilisation (cf. le traitement).

(16) Selon le sens commun, la diffusion suppose la propagation dans diverses directions. Elle implique donc que l'information soit transmise à un large public. La proposition de Directive européenne parle quant à elle de « communication par transmission, diffusion ou toute autre forme de mise à disposition » (art. 2. b).

(17) Le fait que la notion de « communication » ne reçoit pas une définition *ad hoc* posera d'ailleurs de nombreux problèmes; sur ce point voy. *infra*, n° 46.

(18) Sur cette question voy. Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445/2, pp. 15, 16, 18 à 20, 57, 65 et 66; sur ce point voy. en France, à propos de l'expérimentation d'un système de télésurveillance et de sécurité par la R.A.T.P., C.N.I.L., *Douzième rapport d'activités-1991*, Paris, La Documentation française, 1992, pp. 157 et 158; pour d'autres exemples relatifs à des systèmes de sécurité vidéo expérimentés par les collectivités locales françaises voy. *idem*, pp. 183 et s.

(19) Pour une liste exhaustive des utilisations de données retenues par la C.N.I.L. , voy. M. Guibal, Ch. Le Stanc, L. Rapp, M. Vivant, *op. cit.*, n° 1152; J. Frayssinet, *op. cit.*, p. 37 spéc. n° 91.

(20) Voy. l'article 2. c, de la proposition de directive européenne et l'exposé des motifs (inédit), p. 9.

(21) Sur l'impasse tant intellectuelle que pratique de cette « pseudo-distinction » telle que pressentie en jurisprudence et doctrine françaises voy. J. Frayssinet, « La Cour de cassation et la loi informatique, fichiers et libertés, ou comment amputer une loi tout en raffermissant son application », *J.C.P.*, 1988, I, n° 3223; « Contre l'excessive distinction entre fichier et dossier - Le pas en avant du tribunal correctionnel de Paris », *Expertises*, 1990, pp. 16 à 22; note sous T.G.I. Nantes, 16 déc. 1985, *D.*, 1986, I, p. 471; Note sous T.G.I. Créteil, 10 juill. 1987, *D.*, 1988, J., pp. 319 à 323; en ce sens, voy. également G. Bressaud, P. Dan, V. Haddad, A.-C. Kirkam, M.-L. Marie, « D'informatique et libertés à fichiers et libertés », *Expertises*, mars 1991, n° 137, pp. 97 et s.; *contra* : R. Gassin, « Un cas exemplaire de dérive jurisprudentielle du droit pénal technique : l'arrêt de la Chambre criminelle du 3 novembre 1987 relatif aux délits en matière d'informatique, de fichiers et de libertés », *Cahiers du droit de l'informatique*, B, 1988, p. 34, n° 16; « Commentaire du jugement du tribunal correctionnel de Paris du 2 mars 1989 ou, de la distinction des fichiers nominatifs et des dossiers individuels », *Cahiers du droit de l'informatique*, août 1989, E, pp. 3 à 11; (en jurisprudence) voy. Cass. fr. (ch. crim.), 3 nov. 1987, *D.*, 1988, I, p. 17 et note H. Maisl; T.G.I. Nantes, 24 juin 1986, *D.*, p. 471 et note J. Frayssinet; T.G.I. Créteil, 10 juill. 1987, *D.*, 1988, J., pp. 319 à 323 et note J. Frayssinet; Trib. corr. Paris (17e ch.), 2 mars 1989, *Cahiers du droit de l'informatique*, juin 1989, n° 4, D, pp. 26 et 27; pour une critique similaire en droit belge, voy. P. Dejemeppe, « 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.*, janv. 1992, n° 14, p. 893.

(22) C'est d'ailleurs ce qui découle de l'acception logique du terme tel qu'il est défini dans le Petit Robert, c'est-à-dire comme *« un ensemble de pièces relatives à une affaire et placées dans une chemise; la chemise, le carton qui les contient »*.

Il aurait sans doute été plus judicieux de suivre la solution retenue par la proposition de directive européenne. Si ce texte exige également un niveau suffisant de structuration (23), il n'impose pas de finalité de consultation systématique. La définition européenne se concentre, en effet, sur l'accessibilité des données en vue de faciliter leur utilisation ou leur rapprochement. Cette précision donne toute sa valeur au critère en cause, car c'est bien plus dans la *facilité d'utilisation* des données que dans celle de la *consultation* que résident les véritables risques d'atteinte à la vie privée.

On ne comprend d'ailleurs pas ce qui justifie l'exclusion des dossiers du champ d'application de la loi. Le danger pour l'individu est parfois tout aussi réel lorsque l'information qui le concerne est rangée dans un dossier (24). De plus, il existe un risque de voir des dossiers utilisées dans le seul but de détourner la loi; ceux-ci pourraient ainsi regrouper les données dont le traitement est interdit. Il est vrai que les charges administratives qui découleraient de leur inclusion pleine et entière dans le champ de protection paraissent disproportionnées par rapport aux risques qu'ils présentent généralement. La solution était alors à trouver dans l'allégement du système de protection.

13. — Aux termes de l'article 1er, § 4, de la loi, on entend par « tenue d'un fichier manuel » l'enregistrement, la conservation, la modification, l'effacement, la consultation ou la diffusion de données à caractère personnel sous forme d'un fichier sur un support non automatisé.

L'illogisme qui consiste à opposer le traitement automatisé à la tenue d'un fichier manuel a déjà été souligné (voy. *supra*). Il semble avoir été pressenti par le législateur. En effet, la définition de la « tenue d'un fichier manuel » apparaît comme un étrange amalgame des concepts traditionnels de fichier et de traitement.

Cette définition s'apparente à celle du traitement automatisé. La tenue d'un fichier manuel est aussi constituée de diverses opérations effectuées sur des données à caractère personnel. Elle s'en écarte cependant par l'exigence d'organisation des données en fichier sur un support non automatisé.

14. — On peut clarifier la notion de « tenue d'un fichier manuel » en soulignant que son existence est soumise à trois conditions :

— Les données à caractère personnel doivent être organisées sous forme d'un fichier;

— Elles doivent faire l'objet d'au moins une des opérations prévues (25).

(23) Au sens de l'article 2. c, de la proposition de directive, il faut entendre par fichier « tout ensemble structuré de données à caractère personnel, centralisées ou réparties sur plusieurs sites et accessibles selon des critères déterminés ayant pour objet ou pour effet de faciliter l'utilisation ou le rapprochement de données relatives à la ou aux personnes concernées ».

(24) Le législateur l'a lui-même admis (Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1990-1991, n° 1610/1, pp. 4-5). Il élude, toutefois, le problème en décidant qu'il devra faire l'objet de législations spécifiques.

(25) Elles sont identiques à celles prévues dans la définition du traitement automatisé.

De façon étrange, le critère de distinction entre les différents fichiers manuels ne paraît plus être la finalité poursuivie, comme pour les traitements automatisés. En effet, les opérations ne doivent pas constituer un *ensemble*. Le critère semble résider ici dans un élément matériel, le support utilisé (26). L'identification du support pose il est vrai moins de problèmes du fait de la nature même de ces fichiers; on ne se sert pas d'une mémoire informatique mais d'un outil aux contours mieux limités (fiches papier, etc.);

— Les données doivent être conservées et utilisées sur un support non automatisé. Il s'agit selon nous de soumettre à la loi les utilisations de données qui ne s'effectuent pas par le biais d'une technologie de l'information « avancée » (informatique, télématique, etc.). On vise ainsi toute technique qui ne nécessite pas l'emploi d'une machine « intelligente » pour effectuer des opérations sur les données. En ce sens, le support permet un accès direct de l'opérateur à l'information et ce, de manière autonome (la feuille de papier et la microfiche) (27).

1.1.3. — *Le maître du fichier, le gestionnaire du traitement et l'agent traitant*

1.1.3.1. — *Le maître du fichier.*

1.1.3.1.1. — *La définition.*

15. — La loi belge est censée se conformer à la Convention n° 108 du Conseil de l'Europe (cf. *supra*, n° 1). Celle-ci n'arrête pas une définition complète du concept de « maître du fichier ». Elle confie aux lois nationales la mission de déterminer la personne physique ou morale, l'autorité publique ou tout autre organisme compétent pour décider des finalités, des catégories de données enregistrées et des opérations qui leur seront appliquées (28). La Convention laisse donc aux Etats membres le choix des critères déterminant cette compétence.

L'article 1er, § 6, de la loi définit le concept de maître de fichier. Celui-ci est identifié comme « la personne physique ou morale ou l'association de fait compétente pour décider de la finalité du traitement ou des catégories de données devant y figurer ». Toutefois, lorsqu'une loi particulière vient elle-même déterminer un de ces deux éléments, le maître du fichier est la personne physique ou morale que cette loi désigne pour tenir le fichier. Hors de cette hypothèse, la loi n'offre d'autre critère que de rechercher dans les faits qui détient la compétence.

16. — L'identification du maître du fichier à la lumière des deux critères prévus par la loi pourrait donner lieu à des controverses. En effet, bien que la loi établisse que le maître du fichier est la personne « compétente pour décider de la finalité du traitement ou des catégories de données devant y figurer », cette appréciation demeure une pure question de fait. La recherche de la personne compétente risque d'être difficile; les réalités économiques contemporaines favorisent en effet le partage des responsabilités (29). Ainsi, il y a fort à parier que, si un conseil d'administration décide de la création d'un traitement et, partant, de sa finalité, la mise en œuvre de cette décision — et en particulier la détermination des catégories de données — sera dévolue à d'autres instances de l'entreprise. Une requalification pourrait être envisagée dans l'hypothèse où la personne présentée comme maître du fichier n'a pas le pouvoir de décision visé par la loi. Cette source d'insécurité juridique est d'autant plus préjudiciable que l'efficacité du système de protection mis en place par la loi repose sur la détermination d'un responsable unique clairement identifié (30). Seule l'hypothèse où une seule et même personne est compétente pour décider et de la finalité et des catégories de données, lève toute ambiguïté.

Finalement, le seul critère de la compétence de décision quant à la finalité du traitement eût été suffisant. Y associer le critère de la compétence de détermination des catégories de données paraît superflu (31). Par ailleurs, ne garder que la finalité comme moyen d'identifier le maître du fichier est conforme à la ratio de la protection mise en place. La loi vise à concilier deux intérêts contradictoires : l'intérêt poursuivi par celui qui traite les données et l'intérêt de la personne concernée. Dans le cadre de l'activité qu'il exerce ou de la mission qu'il remplit, le ficheur poursuit une finalité qui justifie le traitement de données. En conséquence, c'est à lui de respecter l'équilibre demandé par la loi.

1.1.3.1.2. — *Les missions du maître du fichier.*

17. — Le maître du fichier est le responsable du traitement devant la loi. La centralisation de la responsabilité dans son chef découle du prescrit législatif. Désireux d'assurer aux intéressés une protection efficace de leurs droits, le législateur met expressément à la charge du maître diverses obligations, telle celle de donner suite à l'exercice des droits d'accès et de rectification (32). De même, il est désigné seul responsable des mesures concernant la gestion du traitement (33), la déclaration des traitements automatisés (34), etc. Dans un certain nombre d'hypothèses, la loi s'abstient de désigner un destinataire précis de ses dispositions (35). Si

(26) Il n'empêche que ces fichiers sont également soumis au principe de finalité.

(27) Certes, dans ce cas, l'utilisation d'une « machine » est nécessaire pour accéder à l'information. Ce procédé ne peut cependant pas être considéré comme un support automatisé; il consiste en une simple loupe mais ne permet pas en lui-même de traiter les données.

(28) Voy. article 2. d, de la Convention n° 108 du Conseil de l'Europe.

(29) Voy. sur ce point M. Delmas-Marty, « Le droit pénal, l'individu et l'entreprise : culpabilité "du fait d'autrui" ou du "décideur" ? », *J.C.P.*, 1985-I, n° 3218, 1.

(30) Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445/2, p. 52.

(31) D'autant que le principe de finalité implique que les données soient pertinentes, adéquates et non excessives par rapport à la finalité choisie (voy. *infra*, nos 42 et 43). Le choix des données est donc intrinsèquement dépendant du choix de la finalité.

(32) Articles 10, § 1er et 12, §§ 2 et 3.

(33) Article 16.

(34) Article 17, § 1er.

(35) Notons par exemple le respect du principe de finalité (article 5) et l'interdiction du traitement de certaines données (articles 6 à 8).

ces prescrits s'adressent alors à tous, le maître du fichier supporte là encore une responsabilité particulière, eu égard à son obligation générale de contrôle et de surveillance dans la gestion du traitement (36). Remarquons que, dans toutes ces hypothèses, l'incrimination pénale vise spécifiquement le maître du fichier (37).

18. — Si le maître du fichier est le principal responsable du traitement, il est aussi l'interlocuteur privilégié des personnes concernées par les données et de la commission de contrôle. C'est au maître du fichier que les personnes concernées s'adressent en vue d'exercer leurs droits d'accès et de correction (38).

1.1.3.2. — *Le gestionnaire du traitement et l'agent traitant.*

19. — L'article 1er, § 7, de la loi définit le « gestionnaire du traitement » comme « la personne physique ou morale ou l'organisme non doté de la personnalité juridique à qui sont confiées l'organisation et la mise en œuvre du traitement » (39). Le texte paraît viser par là la personne qui assure concrètement la mise sur pied et le suivi du traitement. Cette personne ne se confond pas avec le maître du fichier, même si celui-ci pourrait assumer les deux fonctions. Il semble bien, à la réflexion, que le seul but visé par cette définition soit très précisément de distinguer le gestionnaire du maître du fichier. Ce dernier reste le principal responsable devant la loi, même si la mise en œuvre et l'organisation du traitement sont confiées à un gestionnaire (40).

20. — La définition du « gestionnaire du traitement » couvre deux réalités distinctes. D'une part, elle vise la personne physique qui, agissant sous la supervision du maître du fichier, est chargée d'exécuter ses décisions et d'assurer la mise en œuvre et le suivi du traitement. D'autre part, elle désigne aussi une personne extérieure à l'organisation, qui preste un service en faveur du maître du fichier. Cet intervenant est communément appelé agent traitant. La plupart des législations étrangères, en ce compris le projet de directive européenne, distinguent ces deux acteurs.

21. — Puisque la loi n'opère pas de distinction entre le gestionnaire agissant en tant que préposé ou mandataire du maître du fichier et l'agent traitant, le même régime devrait s'appliquer aux deux acteurs. L'agent traitant n'est donc tenu d'aucune obligation particulière si ce n'est celles qui ne sont pas mises à la charge exclusive du maître du fichier et qui doivent être observées par tous (respect de la finalité choisie, par exemple).

Cette absence de responsabilité se comprend dans le chef du gestionnaire, personne physique, exerçant ses missions sous le contrôle direct du maître du fichier. Elle se justifie moins en ce qui concerne l'agent traitant. En effet, celui-ci exerce son activité hors de l'entreprise et ne peut donc être contrôlé par le maître du fichier. Bien sûr, le droit commun de la responsabilité délictuelle trouvera à s'appliquer en cas de négligence ou de malveillance de sa part. Et, dans ses rapports avec l'agent qu'il a choisi, le maître du fichier pourra, le cas échéant, mettre en jeu la responsabilité contractuelle. On peut regretter, toutefois, que la loi n'ait pas envisagé de façon spécifique le rôle de l'agent traitant. Un partage de responsabilité, dans l'hypothèse où la gestion du fichier est confiée à un tiers (41), aurait incité tous les acteurs à tenir compte de la protection mise en place.

22. — Remarquons qu'au plan pénal, si le gestionnaire-préposé (ou mandataire) peut être poursuivi en cas de faute personnelle, il n'en est pas de même pour l'agent traitant. En cas de violation de la loi, l'incrimination pénale vise généralement le maître du fichier, son représentant, son préposé ou son mandataire. L'agent traitant n'est ni mandataire du maître du fichier, ni son préposé. Il ne pose aucun acte juridique pour le compte et au nom du maître; il n'agit pas non plus dans un lien de subordination vis-à-vis de celui-ci.

Il semble en conséquence que l'on doive conclure à son immunité pénale (42). Une telle différence de régime paraît difficilement compréhensible. Le travail exécuté par l'agent traitant sera bien souvent identique à celui du gestionnaire-préposé. Les risques d'atteinte aux droits de l'individu sont présents dans les deux hypothèses.

1.2. — **Le champ d'application** *ratione materiae*

23. — Le champ d'application *ratione materiae* de la loi est particulièrement vaste. Il englobe en effet tout traitement de données qu'il soit automatisé ou qu'il s'agisse de la tenue d'un fichier manuel.

24. — L'article 3, § 2, prévoit cependant quatre exceptions. La loi ne doit pas s'appliquer :

— lorsque les traitements, gérés par des personnes physiques, sont, de par leur nature, destinés à un usage privé, familial ou domestique et conservent cette destination. Les conditions de cette exception doivent être bien comprises. Ainsi, seuls les traitements tenus à titre privé par des personnes physiques sont visés. A partir du moment où ils sont mis en œuvre dans le cadre de l'activité professionnelle, ils tombent dans le champ de la loi. Cette exception, qui vise essentiellement les fichiers d'adresses privés (agenda), témoigne du souhait du législateur de ne point interférer dans le cadre strict de la vie privée (43);

— lorsque des traitements portent *exclusivement* sur des données à caractère personnel qui font l'objet d'une publicité en vertu d'une disposition légale ou réglementaire. Il s'agit des traitements de données extraites des déclarations de faillite en nom personnel, des registres de l'état civil, de la conservation des hypothèques, des décisions de justice conservées au greffe, etc. La portée de cette exception est toutefois limitée; seules ces données doivent faire l'objet du traitement.

On voit mal ce qui justifie une exclusion totale du champ d'application. Le risque d'atteinte à la vie privée provient plus de l'utilisation des données que de leur nature. Le fait qu'elles soient soumises à publicité répond à une volonté précise — assurer la sécurité des tiers, par exemple — qui légitime la brèche ouverte dans la vie privée des personnes concernées. L'équilibre ainsi assuré entre des intérêts contradictoires risque d'être remis en question au cas où les données en cause seraient utilisées dans un but différent de celui initialement prévu par la loi ou le règlement. C'est pourquoi, il eût été préférable de soumettre ces données au principe de finalité (44); par ce fait, tout traitement poursuivant une finalité différente de celle pour laquelle la publicité est instaurée aurait dû respecter le prescrit de la loi;

— lorsque des traitements portent exclusivement sur des données à caractère personnel

(36) Article 16.

(37) Voy. *infra*, n° 96.

(38) A cette fin, l'information transmise aux individus lors de la collecte des données ou du premier enregistrement contient les coordonnées du maître. Celles-ci doivent d'ailleurs être transmises à la Commission de la protection de la vie privée qui les consignera avec d'autres informations dans un registre accessible au public. On trouve encore trace de cette volonté dans l'hypothèse où le maître du fichier exerce ses activités de l'étranger; il est tenu soit d'élire domicile en Belgique, soit de s'y faire représenter afin que les personnes concernées puissent exercer leurs droits (art. 1er, § 6, al. 3 et 4).

(39) Il est présenté maladroitement par le ministre dans les documents parlementaires comme couvrant « toutes les délégations qui peuvent être données par le maître du fichier » (Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, 413/12, p. 21). L'expression est malheureuse. On ne saurait viser ici une véritable délégation des pouvoirs de décision du maître du fichier. Si tel était le cas, le délégataire devrait être considéré comme le véritable maître du fichier.

(40) Cela fut confirmé par une réponse du ministre responsable à un membre de la Commission de la Justice qui désirait prévoir un partage de la responsabilité concernant la gestion du traitement (article 16 nouveau) entre les deux fonctions (Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Ch repr., sess. extr. 1991-1992, 413/12, pp. 57 et 58); il faut remarquer qu'aucune infraction pénale ne vise spécifiquement le gestionnaire du fichier, si ce n'est comme préposé ou mandataire.

(41) Un tel système existe en Allemagne (voy. la section 11 de la Bundesdatenschutzgesetz), 20 décembre 1990, Bundesgestezblatt, I, 1990, pp. 2954 et s.). Outre une obligation de sécurité sanctionnée pénalement, la loi allemande prévoit que l'« agent traitant » est le cas échéant soumis à l'obligation de déclarer les traitements qu'il gère pour autrui (art. 32) et doit nommer en son sein un *Beauftragte für den Datenschutz* (commissaire chargé du contrôle interne de la loi); la proposition de directive prévoit également un régime particulier, même s'il s'agit plutôt d'une réglementation du contrat passé entre l'agent traitant et le maître du fichier (art. 24).

(42) Hors les trois cas où l'incrimination pénale est générale (voy. *infra*, n° 98).

(43) Commentaire des articles, *Doc. parl.*, Ch. repr., sess. extr. 1990-1991, n° 1610/1, p. 7; Pour plus de précisions sur ce point voy. F. Robben, « 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, p. 201, n° 3.

(44) Voy. dans le même sens l'avis de la Commission de la protection de la vie privée du 12/05/1992 (*Doc. parl.*, Ch., sess. extr. 1991-1992, n° 413/12, p. 85).

relatives à des individus qui en assurent ou en font assurer la publicité, pour autant que ces traitements respectent la finalité de cette publicité. Selon le ministre responsable du projet de loi (45), la publicité envisagée peut être tant professionnelle (données issues de réclames publicitaires, d'en-tête de lettres, etc.) que personnelle (données issues de faire-part de naissance, mariage, avis nécrologique, etc.). Puisque la finalité de la publicité doit être respectée, la portée de cette exception sera, en pratique, fort limitée. Dans l'hypothèse d'un envoi de faire-part de naissance, il est difficile pour une société de prêt-à-porter pour enfant traitant ces données à des fins de marketing-direct de prétendre poursuive la finalité de publicité initiale;

— lorsque des traitements de données à caractère personnel sont effectués conformément à la loi du 4 juillet 1962 relative à la statistique publique. Celle-ci contient en effet quelques dispositions protégeant la vie privée des individus (46). On est loin cependant de la protection accordée par la nouvelle loi.

On ne comprend pas bien ce qui justifie une telle exception. Elle avalise pour les statistiques publiques un régime de protection plus faible que celui réservé aux statistiques opérées par le privé. Il faut remarquer que lorsque les résultats statistiques permettent la divulgation de situations individuelles, ils ne peuvent être communiqués à des tiers que moyennant le consentement des personnes concernées (47). Si celles-ci refusent, l'I.N.S. peut toutefois les communiquer confidentiellement à certaines administrations publiques (48), mais cette hypothèse, explicitement prévue par la loi, fait tomber leur traitement dans le champ de celle-ci.

1.3. — **Le champ d'application** *ratione personae*

25. — De façon générale, toute personne physique, morale ou association de fait traitant des données à caractère personnel est tenue au respect de la loi. Les professions libérales, les sociétés civiles ou commerciales, les administrations publiques, les établissements scolaires ou universitaires, la presse (49), voire de simples personnes physiques seront, le cas échéant, amenées à se poser la question de l'applicabilité de la loi aux traitements de données qu'ils mettent en œuvre.

26. — Les dispositions de la loi couvrent tant le secteur public que le secteur privé. Le législateur ne fait aucune distinction entre les deux secteurs (50). Il semble ne s'être pas arrêté à la spécificité de nature et de fonctionnement des traitements informationnels développés dans le secteur public. Les fichiers publics se caractérisent en effet par leur exhaustivité (ils portent sur l'ensemble de la population ou sur la totalité d'une catégorie de citoyens) et leur mode de création, qui repose sur une décision unilatérale contraignante issue de l'autorité publique plutôt que sur une relation contractuelle libre entre le ficheur et le fiché (51).

Tout exercice de compétences au sein du secteur public repose sur les principes de légalité, de spécialité et de proportionnalité. Selon ces deux derniers principes tout organisme public désireux d'enregistrer et de traiter des données ne peut le faire que dans la mesure où cela rentre dans la mission qui lui a été confiée (principe de spécialité) et que pour autant que cela lui est nécessaire (principe de proportionnalité) (52).

Si ces deux exigences sont pleinement rencontrées par le texte de la loi (53), le troisième principe de fonctionnement démocratique des pouvoirs publics, le principe de légalité, ne s'y retrouve pas (54). Il n'eût pourtant pas été superflu de préciser de façon explicite que les missions invoquées par une autorité publique pour justifier le traitement d'informations doivent lui avoir été confiées par ou en vertu d'une loi. Le développement des ressources et des circuits informationnels au sein du secteur public augmente en effet les pouvoirs d'action de l'exécutif. Que ce phénomène échappe à la connaissance et au contrôle du législatif et voici l'équilibre des pouvoirs mis en cause (55).

27. — Un régime particulier est prévu pour deux administrations spécifiques, la Sûreté de l'Etat et le Service général du renseignement et de la sécurité (56). Même si elles ne bénéficient pas d'une exclusion totale du champ d'application, ces administrations sont soumises à un très large régime dérogatoire. Elles échappent ainsi aux dispositions censées incompatibles avec l'exercice de leurs missions. Il s'agit principalement des droits d'information, d'accès direct (57) et de rectification de la personne concernée et des dispositions relatives aux données « sensibles » (58).

1.4. — **Le champ d'application** *ratione loci*

28. — La loi précise les limites territoriales de ses effets. Après l'analyse du principe général, nous nous pencherons succinctement sur les flux transfrontières de données.

1.4.1. — *Le principe général*

29. — La loi opère une distinction entre la tenue d'un fichier manuel et la mise en œuvre d'un traitement automatisé. Aux termes de l'article 3, § 1er, la législation s'applique lorsque le fichier manuel est établi en Belgique. Le critère de l'application territoriale est, dans ce cas, la situation matérielle du fichier. La nature même de ce type de fichier, composé généralement de fiches en papier sur lesquelles sont reprises les informations, permet sa localisation physique, si bien que le critère retenu ne devrait pas susciter de difficulté.

30. — La localisation des traitements automatisés est plus complexe. Les progrès de la technologie conduisent en effet à un éparpillement sans cesse croissant des opérations du traitement sur le territoire de différents Etats. Ainsi, la collecte de données à caractère personnel peut avoir lieu dans les pays A et B; ces données transitent via un réseau par le territoire d'un pays C, pour être traitées dans un pays D; elles sont ensuite réimportées dans les pays A et B, voire dans d'autres Etats. Quelles sont alors les lois susceptibles de s'appliquer aux traitements en cause ? La loi tente d'apporter une réponse à cette question.

31. — L'article 3, § 1er, 2°, déclare la loi applicable « à tout traitement automatisé, même si tout ou partie des opérations est effectué à l'étranger, pourvu que ce traitement soit directement accessible en Belgique par des moyens propres au traitement ».

La loi appréhende deux situations différentes. Soit l'ensemble des opérations constitutives du traitement automatisé « se situent » en Belgique, soit tout ou partie de celles-ci sont localisées à l'étranger. Dans la première hypothèse, la loi belge s'applique naturellement. Dans la seconde hypothèse, la solution retenue par le législateur peut surprendre. Face à une situation affectée d'un élément d'extranéité, il déroge au système des règles de conflit bilatérales. Il ne fournit pas un critère de choix de la loi applicable, mais établit une règle de droit international privé matériel, « norme qui saisit une situation internationale typique et la soumet à des règles appropriées » (59). Le problème ne sera pas de rechercher quelle loi vont appliquer les auto-

(45) *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, n° 413/12, p. 26.

(46) Voy. spécialement les articles 2, 15, 18 et 24*quinquies* (ce dernier article ne vise cependant que l'Institut national de statistique). Il est à remarquer que cette protection reste aussi en deçà des mesures proposées par la Recommandation n° R (83) 10 du Conseil de l'Europe relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques.

(47) Article 2, c, al. 1er, de la loi du 4 juillet 1962, *M.B.*, 20 juill. 1962.

(48) Article 2, c, al. 2, de la loi du 4 juillet 1962.

(49) Voy. Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445/2, pp. 59 et 63.

(50) Dans sa première version, la proposition de directive européenne distinguait très nettement les secteurs public et privé, prévoyant pour ce dernier un régime de loin plus exigeant que pour le premier. Lors de la révision du texte, cette différence fut abandonnée.

(51) M.H. Boulanger et C. de Terwangne, « 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, pp. 6-7.

(52) Dans le même sens voy. Th. Léonard et Y. Poullet, « 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, 1992, p. 242, n° 15 (voy. aussi, n° 51).

(53) Voy. *infra*, le principe de finalité applicable tant aux secteurs public que privé.

(54) Si ce n'est pour les données sensibles et indépendamment du secteur en cause (voy. *infra*, n°s 52 et s.).

(55) M.H Boulanger, et C. de Terwangne, *op. cit.*, p. 7.

(56) Article 3, § 3, al. 1er.

(57) Une procédure d'accès indirect est prévue à l'article 13, 2°.

(58) Pour une vision critique de ce régime voy. F. Rigaux, « La protection de la vie privée à l'égard des données à caractère personnel », *Annales de droit de Louvain*, 1993/1, pp. 59 et s.

(59) F. Rigaux, « Le régime des données informatisées en droit international privé », *Journ. dr. intern.*, 1986, p. 316, n° 8.

rités chargées du contrôle de la réglementation, mais bien à quels faits la loi belge s'applique (60). Celle-ci se présente donc comme une « loi d'application immédiate » (61) : le domaine spatial des règles de protection est impératif; il force la compétence de l'ordre juridique belge (62).

32. — La solution énoncée par le législateur se comprend aisément. La loi relève en partie, par son objet, du droit administratif. Non seulement elle met en place des sanctions pénales, mais le système de protection se base sur l'existence d'une autorité administrative chargée d'en contrôler l'application (63). Dès lors, ce caractère administratif va rejaillir sur la solution du conflit de loi (64). L'autorité de contrôle mise en place a vocation à n'appliquer que son propre droit. Elle ne remplira ses missions que dans les situations de fait tombant sous le critère de rattachement édicté par sa loi nationale (65).

33. — Le critère de rattachement proposé par la loi réside dans l'accès au traitement. Tout traitement accessible en Belgique tombe sous le coup de la loi, pourvu qu'une double condition soit remplie :

— 1° l'accès au traitement doit être direct;

— 2° l'accès doit se faire par des moyens propres au traitement.

Lors des débats en Commission de la justice (66), le ministre a précisé que, par ces critères, on visait tout traitement accessible par un opérateur, en Belgique, sans qu'une autre intervention humaine ne soit nécessaire. Ainsi, « si un traitement est accompli par un ordinateur situé en Allemagne et si un opérateur peut au départ du territoire belge consulter ou agir sur ce traitement sans l'intermédiaire d'une autre personne en Allemagne, on pourra dire que le traitement est directement accessible en Belgique par des moyens propres au traitement ». Par contre, les critères retenus ne seront pas satisfaits si « l'opérateur établi en Belgique téléphone à un collègue en Allemagne qui, lui, dispose d'un terminal permettant d'accéder au système ». Il ajoute que les moyens mis en œuvre pour consulter les données (lignes téléphoniques ordinaires, réseaux privés, P.C., Minitel, etc.) sont sans influence sur le critère de rattachement (67).

34. — S'ils sont accessibles suivant les modalités analysées ci-avant, les traitements mis en œuvre à l'étranger tombent dans le champ d'application territoriale de la loi. Contrairement à certaines législations étrangères, ce n'est pas alors uniquement dans le chef de l'utilisateur que la loi s'applique (68), mais bien dans le chef du maître du fichier étranger. Par là, on reconnaît une compétence extra-territoriale à la Commission de protection de la vie privée. Le maître du fichier étranger qui désire écouler des données à caractère personnel sur notre territoire doit respecter la réglementation belge in extenso; il doit donc s'établir en Belgique, introduire une déclaration, prévoir un droit d'accès, gérer son traitement suivant les règles énoncées à l'article 16, etc. S'il ne remplit pas ces obligations, son traitement devra être considéré comme illicite... (69).

35. — Se pose alors le problème de l'effectivité de la protection mise en place par la loi belge. Comment contrôler son respect à l'étranger ? Les autorités administratives belges ne peuvent en effet exercer un contrôle au-delà des frontières (70). Que se passera-t-il si le maître du fichier étranger refuse de se conformer à la loi parce que, par exemple, le traitement mis en œuvre est tout à fait conforme à sa loi nationale ? (71).

A la réflexion, le législateur a perdu de vue la seule règle qui autorise un contrôle efficace des traitements automatisés de données : la protection ne peut s'appliquer qu'aux éléments du traitement matériellement localisés sur le territoire belge (72). Il n'était pas nécessaire de soumettre à la loi belge le traitement automatisé entièrement effectué à l'étranger, mais accessible depuis la Belgique. On pouvait, sur le modèle luxembourgeois, imposer à *l'interrogateur* belge de respecter la loi pour ce qui le concerne, et le charger en conséquence de déclarer les données obtenues et insérées dans son traitement. Ou encore ne permettre les flux que moyennant une autorisation préalable (73) délivrée sous réserve d'un contrôle des données importées et de la légitimité de leur utilisation par l'importateur. Dans ces deux hypothèses, ce ne serait pas le maître du fichier étranger qui serait soumis à la réglementation belge, mais bien l'importateur belge. Un contrôle efficace de l'utilisation ultérieure des données à caractère personnel importées serait dès lors possible.

1.4.2. — *Les flux transfrontières de données*

36. — La question capitale des communications de données à caractère personnel effectuées vers l'extérieur du territoire national a été largement éludée par la loi. Aux termes de l'article 22, les flux transfrontières de données peuvent être soit interdits, soit soumis à autorisation préalable, soit réglementés, en vue d'assurer le droit au respect de la vie privée. Le texte de la loi s'en tient là et confie au Roi le soin de régler le sort de ces flux de données vers l'étranger. Seule la collecte a retenu l'attention du législateur. L'article 4, § 2, interdit la collecte de données dites « sensibles » lorsque celles-ci sont destinées à être traitées à l'étranger.

La réglementation des flux transfrontières doit être respectueuse des engagements internationaux pris par la Belgique (74). Il s'agit dès lors d'observer les principes mis en place par la Convention de 1981 du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. L'article 12 de cette Convention prévoit que les Etats contractants (75) ne peuvent mettre de barrières aux transmissions de données aux seules fins de la protection de la vie privée. La Convention admet différentes exceptions à ce principe. Une partie contractante peut notamment restreindre les flux de données pour lesquelles elle a prévu une régle-

(60) En ce sens voy. B. Hanotiau, « Les flux transfrontières et la problématique du droit international privé », *in La télématique - Aspects techniques, juridiques et socio-politiques*, Gand, Story-Scientia, t. II, 1985, p. 187, n° 30.

(61) F. Rigaux, *op. cit.*, n° 8.

(62) P. Mayer, « Les lois de police étrangères », *Journ. dr. intern.*, 1981, p. 284, n° 10.

(63) De plus, il se peut que le maître du fichier soit une administration publique.

(64) B. Hanotiau, *op. cit.*, p. 187, n° 30.

(65) *Idem*, n° 16.

(66) Discussion, article par article, au sein de la Commission de la justice de la Chambre, *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, n° 413/12, p. 22.

(67) On peut se poser la question de la pertinence de tels critères. Si l'on veut garantir la protection de la vie privée des individus, même si les données qui les concernent proviennent de l'étranger, pourquoi l'accorder seulement lorsqu'elles sont directement accessibles par des moyens propres au traitement ? Certes, l'atteinte est ainsi facilitée mais l'accès indirect aux données peut engendrer les mêmes conséquences néfastes pour les personnes concernées.

(68) Voy. l'article 3 (3), alinéa 2, de la loi luxembourgeoise (Loi réglementant l'utilisation des données nominatives dans les traitements informatiques, 11 avril 1979, *Mémorial*, A, n° 29, 11 avril 1979) qui énonce que « si une banque de données, implantée sur un territoire étranger, est accessible au Grand-Duché de Luxembourg au moyen d'un terminal, les prescriptions de la présente loi doivent être observées par l'utilisateur de ce terminal ».

(69) Il faut remarquer que les conséquences de cette disposition risquent d'être contraires à la future directive européenne. L'article 4.1 établit que « chaque Etat membre applique les dispositions de la présente directive à tous les traitements de données à caractère personnel : *a*) dont le responsable est établi sur son territoire ou relève de sa compétence (...) ». Ce texte permet à chaque Etat membre de préciser les conditions de licéité d'un traitement. Toutefois, cela n'autorise pas un Etat à contrôler les traitements effectués par un responsable résidant dans un autre Etat membre car le respect de la directive sur tout le territoire de la Communauté suppose l'équivalence de protection d'un Etat à l'autre (13e considérant). Obliger le maître du fichier résidant sur le territoire de la C.E.E. à se soumettre à la loi belge reviendrait à éluder ce principe.

(70) F. Rigaux, « Le régime des données informatisées... », *op. cit.*, p. 325, n° 23.

(71) Le ministre lui-même paraît conscient de ces difficultés (voy. Discussion, article par article, au sein de la Commission de la justice de la Chambre, *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, n° 413/12, p. 23). Pourquoi alors ne pas avoir amendé le texte de l'article 3 ?

(72) F. Rigaux, « La loi applicable à la protection des individus à l'égard du traitement de données à caractère personnel », *Rev. crit. dr. intern. privé.*, 1980, p. 469, n° 30.

(73) Cette autorisation ne serait pas contraire à la Convention du Conseil de l'Europe auquel le texte belge est censé se conformer. La libre circulation des données entre Etats signataires n'interdit pas les autorisations à l'importation, mais bien à l'exportation (art. 12, 2). Voy. dans ce sens F. Rigaux, « La loi applicable à la protection des individus... », *op. cit.*, p. 456, n° 16. Transposée dans les réglementations nationales, la directive européenne refusera, par contre, tout contrôle des flux entre Etats membres.

(74) Le texte de la loi le reconnaît expressément : « sans préjudice des conventions internationales auxquelles la Belgique est partie,... » (art. 22).

(75) A savoir, à ce jour, l'Allemagne, l'Autriche, le Danemark, l'Espagne, la France, l'Irlande, l'Islande, le Luxembourg, la Norvège, le Royaume-Uni et la Suède.

mentation spécifique (76). Elle ne peut toutefois recourir à cette possibilité si l'Etat signataire, destinataire des données, prévoit un régime de protection équivalent. La loi belge lorsqu'elle pose à l'article 4, § 2 un principe absolu d'interdiction, est donc en contradiction avec la Convention.

Par ailleurs, la directive européenne en projet vise à assurer la libre circulation des données au sein de la Communauté. En principe, ce texte impliquera de ne plus limiter les flux des données entre Etats membres. Les transmissions à destination de pays tiers devront, quant à elles, respecter le prescrit communautaire : elles ne pourront avoir lieu que si les pays tiers en cause assurent un niveau de protection adéquat (77).

2. — LES LIGNES DIRECTRICES DE LA PROTECTION

37. — L'équilibre instauré par le législateur entre l'intérêt de la société à utiliser et voir circuler l'information et le droit de l'individu de protéger sa vie privée, repose sur le principe fondamental de finalité [2.1]. Analysant dans un premier point la portée de ce principe, nous avons jugé opportun d'y inclure la problématique de la communication des données. La loi n'a pas, en effet, réservé de régime spécifique à la communication et la légitimité de cette dernière nous paraît devoir s'apprécier à la lumière du principe de finalité. Par ailleurs, les auteurs de la loi ont réservé à certaines catégories de données particulièrement révélatrices d'aspects intimes de la personnalité, une protection très stricte [2.2]. Ce sont là les lignes directrices du nouveau régime légal mis en place.

2.1. — Le principe de finalité

2.1.1. — *La portée*

38. — Le principe de finalité constitue la pierre angulaire de toute législation garantissant la protection de la vie privée face aux traitements de données à caractère personnel. Il se fonde sur un postulat fort simple : le danger inhérent aux traitements de données à caractère personnel réside davantage dans les finalités qu'ils poursuivent que dans la nature des données qui en font l'objet. Qu'une personne déclare son appartenance syndicale est une information somme toute anodine dans un Etat démocratique. Selon son contexte d'utilisation, cette donnée s'avérera cependant plus ou moins sensible : tantôt elle permettra à l'individu de recevoir sa convocation au conseil d'entreprise; tantôt elle servira de base à des discriminations intolérables.

39. — L'article 5 de la loi énonce le principe de finalité en ces termes : « 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 par rapport à ces finalités » (78).

Cette disposition pose en fait deux principes distincts (79). Le premier — principe de légitimité — postule que le but du traitement soit déclaré et légitime. Le second — principe de conformité — exige un lien étroit entre l'utilisation des données et la finalité légitime déclarée. Toute utilisation des données doit être compatible avec la finalité. Plus précisément, les données doivent être adéquates, pertinentes et non excessives par rapport à cette finalité.

Il convient de noter ici que la loi ne condamne pas *a priori* les changements de finalité. Elle les autorise, en effet, implicitement pour peu que la nouvelle finalité soit légitime et déterminée (80). La directive européenne en projet est plus sévère sur ce point étant donné qu'elle exige que la modification de la finalité d'un traitement soit compatible avec la finalité annoncée *ab initio* (81).

2.1.1.1. — *Le principe de légitimité.*

40. — Le principe de légitimité obéit lui-même à deux règles. La première, formelle, exige que le but poursuivi par le traitement soit déclaré. Cette exigence de transparence est primordiale. Une finalité secrète qui ne permettrait pas le contrôle de l'utilisation des données en cause est illicite.

41. — La seconde règle a trait à l'objet même de la finalité. Celle-ci doit être légitime. De façon étrange, cette exigence fondamentale n'a fait nulle part l'objet d'une précision. Nous retiendrons ici une interprétation qui se base sur une lecture téléologique du principe de finalité. Si le but de la loi est bien de garantir la protection de la vie privée des individus dans notre société, la finalité du traitement et sa mise en œuvre doivent concilier les intérêts de la personne concernée par les données et l'intérêt général ou l'intérêt particulier poursuivi par le responsable du traitement. Il en résulte qu'une finalité choisie violant les intérêts individuels sans se fonder sur un intérêt supérieur doit être considérée comme illégitime. L'autorité de contrôle et le juge contrôleront cette légitimité sur base de la méthode de pondération des intérêts, reposant sur la règle de proportionnalité. On pourrait admettre, par exemple, que des données très sensibles (concernant, par exemple, les opinions politiques et les habitudes sexuelles) soient traitées par la Sûreté de l'Etat à propos d'individus suspectés de travailler pour une puissance étrangère visant à déstabiliser l'Etat belge. La finalité du traitement — la définition précise du profil de tels individus — se fonde ici sur l'intérêt général de la nation (82). Cet exemple est certes extrême. Il a, cependant, l'avantage de mettre en évidence l'utilité d'un principe qui permettra aux autorités de contrôle de sanctionner les violations flagrantes des droits individuels.

2.1.1.2. — *Le principe de conformité.*

42. — Une finalité légitime et déclarée n'autorise pas d'elle-même l'utilisation de n'importe quelle donnée. Le principe de conformité implique tout d'abord que l'utilisation des données soit compatible avec la finalité légitime et déclarée. Si une entreprise déclare traiter des données en vue de la gestion de son fichier clientèle, cela ne lui permet pas automatiquement de les vendre à une autre entreprise. Pour ce faire, elle devrait déclarer cette autre finalité dont la légitimité serait contrôlée.

Le principe de conformité implique également que les données utilisées soient adéquates, pertinentes et non excessives par rapport à la finalité déclarée et légitime. On retrouve ici explicitement la règle de proportionnalité. L'adéquation et la pertinence de la donnée ne visent rien d'autre qu'une liaison nécessaire et suffisante de l'information au but poursuivi par le traitement. Ainsi, une donnée relative aux habitudes sexuelles d'un individu ne se justifie pas dans un traitement ayant pour finalité la gestion d'un recensement de la population. Elle n'est pas nécessaire à la poursuite de ce but. De même en France, la C.N.I.L. refuse généralement l'accès au numéro d'inscription au Répertoire national d'identification des personnes physiques lorsque cette identification peut être réalisée par d'autres moyens (83). Le caractère non excessif de la donnée exige que même si son utilisation s'avère nécessaire au vu de la finalité poursuivie, elle ne soit pas retenue si elle présente un risque d'atteinte disproportionné aux intérêts individuels de la personne concernée.

43. — Clé de voûte du système de protection mis en place par la loi, le principe de finalité fera l'objet d'un contrôle tant de la part des personnes concernées par les données que de celle des autorités de contrôle. Le cas échéant, le maître du fichier, son représentant, son préposé ou mandataire devront répondre de sa violation devant les juridictions pénales (84).

2.1.2. — *La communication des données*

44. — Si l'on ne peut enregistrer des données à caractère personnel à n'importe quelle fin, ni les traiter de n'importe quelle manière, on ne

(76) Article 12.3.a.; une seconde possibilité de dérogation est prévue lorsqu'un transfert de données est projeté vers le territoire d'un autre Etat contractant, ce dernier pays ne servant que de transit vers un Etat tiers à la convention. Un tel procédé permettrait en effet de contourner la législation du pays d'origine.

(77) Article 26 de la dernière version de la proposition de directive. Des exceptions sont envisagées par le texte, justifiées par le consentement de la personne concernée, l'exécution d'un contrat, ou la sauvegarde d'un intérêt public important ou d'un intérêt vital de la personne concernée (art. 26.1., al. 2).

(78) Remarquons que c'est la première fois que ce principe est consacré dans une législation nationale de manière aussi explicite.

(79) Sur ces distinctions voy. Th. Léonard et Y. Poullet, *op. cit.*, pp. 232 et s., spéc. n^{os} 35 et s.

(80) Article 5. Avant d'effectuer le changement de finalité d'un traitement automatisé, il faut le déclarer à la Commission de protection de la vie privée. Dans le même sens, F. Robben, « Het wetsontwerp Wathelet tot bescherming van de persoonlijke levenssfeer t.o.v. de bewerking van persoonsgegevens », Computerrecht, 1992/1, p. 5.

(81) Article 6 (b) de la proposition de directive.

(82) Pour autant que la poursuite de cet intérêt soit bien réelle.

(83) Voy. par ex., la Délibération n° 90-83 du 26 juin 1990 *in* C.N.I.L., *Onzième rapport d'activité 1990*, Paris, La Documentation française, 1991, p. 190.

(84) Article 39, 3°.

peut pas plus les communiquer à n'importe qui ou pour n'importe quel motif.

Les risques de violation de la vie privée ou d'autres droits fondamentaux des citoyens ne se limitent pas à l'enceinte du service de l'entreprise ou de l'administration qui a enregistré et qui traite des données portant sur les individus. Au contraire, lors du passage à l'extérieur de cette enceinte, les risques sont d'autant plus réels que la personne concernée perd la maîtrise immédiate de l'information qui circule à son propos. Elle n'est plus, en effet, la source directe de son image informationnelle. Dès lors, tenue à l'écart du circuit d'information, elle ignorera l'utilisation qui est faite de ses données, le sort qui leur est réservé au-delà de la communication.

Il est donc primordial, lors de la mise en place d'un régime légal protecteur, d'envisager avec un soin particulier le phénomène de la transmission des données à caractère personnel.

45. — Dans sa liste de définitions préliminaires, la loi ne fait nulle mention de la notion de « communication ». Elle lui préfère deux termes proches mais distincts (qui, paradoxalement, ne réapparaîtront plus dans le texte par la suite...) : la consultation et la diffusion. Ces deux opérations sont considérées comme faisant partie de ce que la loi définit comme « traitement automatisé » (85) ou comme « tenue d'un fichier manuel » (86).

On peut y voir deux formes de communication, l'une à connotation passive, l'initiative étant réservée à celui qui désire avoir accès aux données, l'autre désignant l'envoi des informations vers des points de réception multiples. Il est tout de même regrettable que la communication en tant que telle ne soit pas reprise comme opération constitutive du « traitement » et, surtout, qu'elle ne fasse pas l'objet d'une définition soignée et précise (87). C'est en effet ce terme qui revient à travers le texte (88) et c'est en outre à lui que se ramènent les diverses autres notions utilisées ça et là : transmission, accès, obtention, divulgation.

2.1.2.1. — *La définition de la communication.*

46. — Définir ce qu'il faut entendre par « communication » permettrait de cerner avec précision les lieux et moments de danger accru pour la protection de la vie privée des individus. Par là la possibilité existe de contrôler les flux d'informations.

On l'a déjà dit, ce n'est pas uniquement lors de la transmission des données vers l'extérieur que le danger s'intensifie pour les individus concernés. Un transfert, au sein d'un même organisme ou d'une même administration, entre services accomplissant des missions à finalités différentes, comporte tout autant de risques. Le seuil critique est celui du passage hors de l'orbite d'action et de contrôle du maître du fichier responsable des données enregistrées. C'est en effet lorsque l'on sort du champ de l'autorité directe du responsable du traitement que la maîtrise des données s'amoindrit et que s'accentue le danger de voir les données utilisées à d'autres fins que celles initialement poursuivies.

Ainsi, la transmission des données en-dehors de la sphère d'autorité du maître du fichier s'accompagne d'un changement, voire d'un détournement de finalité, lorsque le service crédit d'une banque transfère son fichier au service responsable de l'activité d'assurance que la banque a éventuellement développée. Ou lorsque l'administration cadastrale transmet à l'administation fiscale les informations qu'elle recueille lors de l'enregistrement des ventes immobilières. De telles communications, qui ne répondent pas au but pour lequel les données avaient été enregistrées, risquent de léser les droits des personnes fichées qui, non averties, ne peuvent se douter des destinataires de leurs données et des opérations effectuées sur celles-ci.

47. — La Commission de la protection de la vie privée propose de comprendre par « communication » : « la diffusion ou la divulgation, la transmission ou la mise à disposition d'une personne physique ou morale de données à caractère personnel ». Elle ajoute surtout : « la communication ne comprend pas la diffusion ou la mise à disposition de données à caractère personnel à d'autres personnes au sein de l'organisation ou de l'entreprise dans laquelle opère le maître du fichier, si ces personnes reçoivent ces données dans l'exercice de leurs fonctions » (89).

Au niveau européen, on retrouve la même préoccupation de déterminer clairement ce qu'il faut entendre par « communication ». L'approche adoptée est toutefois différente. C'est la notion de « tiers » qui a été définie, la communication, perçue comme transmission de données à un tiers, dépendant en effet de cette dernière notion (90). Selon la plus récente version de la proposition de directive, sont à considérer comme « tiers » toutes « personnes physiques ou morales autres que la personne concernée, le responsable du traitement et les personnes habilitées à traiter les données agissant sous son autorité directe ou pour son compte » (91).

Cette deuxième définition rejoint davantage celle qui, à notre sens, reflète au mieux le phénomène « dangereux » qu'il s'agit de circonscrire. Il y a lieu, selon nous, de considérer qu'il y a communication lorsque des données, traitées sous l'autorité d'un responsable, sont transmises à un tiers qui se situe en-dehors de cette autorité (hormis l'agent traitant). La définition de la Commission belge présente à ce point de vue le défaut de ne pas prendre en considération le champ d'action du maître du fichier. Elle n'envisage en effet la communication que dans les rapports avec l'extérieur de l'entreprise ou de l'organisation dans son ensemble.

2.1.2.2. — *Le régime de la communication.*

48. — Pas plus qu'ils ne la définissent avec précision, les auteurs de la loi ne réservent de régime spécifique à la communication.

Il ressort cependant de certaines dispositions du texte que le maître du fichier est tenu de consigner dans l'état qu'il établit pour chaque traitement automatisé dont il est responsable, les personnes ou catégories de personnes à qui les données sont transmises (92). Cette mention doit également se retrouver dans la déclaration que le maître du fichier doit déposer auprès de la Commission de protection de la vie privée préalablement à toute mise en œuvre de traitement automatisé (93). Il lui incombe en outre dans sa gestion des traitements, de veiller à ce que les données à caractère personnel ne puissent être communiquées qu'aux catégories de personnes admises à y accéder (94).

C'est donc au maître du fichier qu'il appartient de décider des destinataires des données. La loi n'apporte aucune indication sur le critère à suivre pour désigner les destinataires. Il semble cependant que la logique veuille que ce soit le principe de finalité qui guide le maître du fichier : communiquer les données à telle ou telle catégorie de personnes s'inscrit-il dans la finalité poursuivie par le traitement ? (95). Il faut distinguer deux types de communications : celles qui constituent une fin en soi et celles qui participent à l'accomplissement d'une finalité distincte (96).

2.1.2.2.1. — *La communication, finalité principale.*

49. — Les communications du premier type se présentent lorsque, par exemple, un chasseur de têtes transmet à son client les informations qu'il a rassemblées sur un « gibier » ciblé ou, plus classiquement, lorsqu'une société de mailing vend à une entreprise les fichiers qu'elle a élaborés. Dans ces deux cas, la finalité de l'activité commerciale mise en œuvre est la communication (avec profit) des données collectées.

Dans la mesure où pareille finalité est parfaitement légitime dans le chef de chacun de ces deux agents économiques, et pourvu qu'elle

(85) Article 1er, § 3 (voy. *supra*, n° 9 pour l'énoncé complet de cette disposition).

(86) S'il s'agit de la consultation ou de la diffusion de données sous forme d'un fichier sur un support non automatisé (art. 1er, § 4).

(87) Voy. en ce sens l'avis de la Commission de la protection de la vie privée n° 10/92 du 20 août 1992, Annexe II au Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Sén., n° 445-2, p. 123.

(88) Articles 7, al. 4 (il est interdit de *communiquer* les données médicales à un tiers), 12, § 3 (nécessité de transmettre les corrections aux personnes à qui communication a été faite), 14, § 1er (demande tendant à faire interdire d'utiliser une donnée dont la *communication* est interdite), 16, § 1er, 5° (le maître du fichier veille à ce que les données ne soient *communiquées* qu'aux personnes autorisées), 17, § 3, 8° (la déclaration doit mentionner les garanties dont doit être entourée la *communication* des données).

(89) Avis du 12 mai 1992, *op. cit.*, n° 413-12, p. 82.

(90) Notons que les précédents projets de loi en la matière recouraient pareillement à la notion de tiers, voy. le projet Gol, *op. cit.*, art. 1er, § 3.

(91) Article 2 (g).

(92) Article 16, § 1er, 1°.

(93) Article 17, § 1er et § 3, 7°.

(94) Article 16, § 1er, 5°.

(95) C'est ce raisonnement qu'effectue la C.N.I.L. lorsqu'elle condamne la transmission du fichier du personnel d'E.D.F. au parti communiste français : dans la mesure où cette transmission sortait de la finalité du fichier elle n'était pas admissible (délibération n° 84-40 du 20 novembre 1984, *J.C.P.*, 1984, I, 13905).

(96) Voy. Th. Léonard et Y. Poullet, *op. cit.*, pp. 264 et s.

soit clairement déterminée (97), elle peut être poursuivie en toute légalité au regard de la législation de protection. La loi s'en tient là mais, à notre sens, pour être admissibles les opérations de communication devraient satisfaire un second test de validité : la finalité du traitement qui bénéficie de la communication devrait, elle aussi, être légitime (98).

La loi, rappelons-le, ne précise pas comment évaluer la légitimité, que ce soit pour établir l'admissibilité de l'ensemble d'un traitement ou d'une simple communication de données. Il semble, néanmoins, opportun de proposer ici un critère qui permette aux justiciables, et le cas échéant aux juges, de s'en remettre à une méthode d'évaluation objective plutôt qu'à l'arbitraire.

La légitimité peut s'établir par référence à une loi qui fonde le traitement ou la communication en cause. Ainsi, les traitements de données effectués au sein du secteur public sont justifiés par les compétences confiées par la loi aux différents organes publics (99). La transmission d'informations ne peut avoir lieu, dans ce cas, que si elle s'inscrit dans l'exécution des tâches relevant de ces compétences. A défaut d'une telle loi, il convient de mettre en balance l'intérêt retiré par le maître du fichier ou le destinataire des données, et celui de l'individu à voir préservés ses libertés et droits fondamentaux, et notamment sa vie privée. Il y a donc lieu d'appliquer le principe de proportionnalité et de vérifier que l'atteinte aux intérêts de la personne fichée ne soit pas excessive (100). L'agent du secteur privé qui désire diffuser un fichier à des fins de marketing, par exemple, doit en conséquence être en mesure de prouver que l'intérêt économique que représente pour lui la circulation commerciale du fichier en question (qui assure le fonctionnement de son entreprise) est supérieur au préjudice que les personnes fichées encourent du fait de la divulgation de données les concernant (les données transmises peuvent éventuellement être de nature *a priori* anodine — noms, prénoms, adresses,... — ou avoir déjà fait l'objet d'une publication). La personne du secteur privé qui, à l'opposé, souhaite obtenir communication de données à caractère personnel, que ce soit en provenance du secteur public ou d'une autre entité privée, doit elle aussi démontrer d'un intérêt supérieur à celui que les sujets des données auraient à s'opposer à la transmission de celles-ci.

50. — Il arrive que l'opération de transmission des informations réalise par elle-même un changement de finalité. Ainsi lorsqu'une administration décide de commercialiser les fichiers qu'elle détient. Les données collectées lors de l'élaboration de ces fichiers ne l'ont certes pas été aux fins d'être disséminées en vue d'un intérêt commercial. La diffusion s'inscrit donc bien dans le cadre d'une finalité totalement différente (celle de tirer un profit économique des données).

Rappelons que la loi ne condamne pas *a priori* ce genre de comportement, pourvu que la nouvelle finalité soit légitime et déclarée et que les données soient pertinentes et non excessives par rapport à cette finalité.

2.1.2.2.2. — *La communication, finalité accessoire.*

51. — La seconde catégorie de communications concerne les transferts accessoires à une autre opération. La communication participe ici à l'accomplissement d'une finalité distincte. C'est le cas de la banque qui, pour effectuer un paiement sur ordre d'un de ses clients, transmet les données nécessaires à un autre organisme financier.

La légitimité de semblable divulgation ne fait généralement aucun doute, ni dans le chef de l'organe communiquant, ni dans celui du récepteur. On peut toutefois soutenir, au-delà de la loi, que le test de proportionnalité a encore sa place et qu'il serait bon de s'interroger sur la nécessité de la communication par rapport au but visé, et sur le caractère excessif ou non de l'atteinte portée par cette opération aux droits et libertés de la personne concernée.

Dans pareil cas, le danger issu de la communication — la dispersion des informations entre diverses mains — est limité : le sujet garde la maîtrise de ses données car il sait qui sait quoi et qui en fait quoi. La communication est (raisonnablement) connue de lui. Le destinataire ne peut, en principe, conserver les données reçues au-delà de la période nécessaire à l'accomplissement du but pour lequel elles ont été transmises (délai de conservation des preuves pour les éventuels cas de contestation, par exemple) (101). Le récepteur de l'information peut, cependant, désirer garder celle-ci plus longtemps, ou l'utiliser à d'autres fins. Il faut alors, pour que ce soit admis, que le but poursuivi soit légitime et que les données en cause soient pertinentes par rapport à ce but. En pareil cas, étant donné la modification de finalité, on doit considérer qu'il y a nouveau traitement des données et le responsable de celui-ci est dès lors tenu d'en informer la personne concernée (102).

2.2. — Le traitement des données « sensibles »

52. — Certaines catégories de données, que la doctrine qualifie généralement de « sensibles » (103), sont soumises à un régime protecteur spécifique (104). Elles recouvrent les données énumérées à l'article 6 de la loi, à savoir les données relatives aux origines raciales ou ethniques, à la vie sexuelle, aux opinions ou activités politiques, philosophiques ou religieuses, aux appartenances syndicales ou mutualistes (105). Il convient d'y adjoindre les données médicales et les données judiciaires répertoriées respectivement aux articles 7 et 8.

2.2.1. — *Les données énumérées à l'article 6 et les données judiciaires*

53. — La première catégorie de données sensibles concerne les données énumérées à l'article 6. Celles-ci ne peuvent être traitées qu'à des *fins déterminées par ou en vertu de la loi* (106). Des conditions particulières peuvent être prévues par arrêté royal (107). Un tel régime nous paraît peu praticable. Faudra-t-il, par exemple, que le législateur intervienne pour autoriser le traitement par les banques des données relatives à une appartenance syndicale, si un individu règle sa cotisation syndicale par virement bancaire ?

54. — La deuxième catégorie concerne les données judiciaires énumérées exhaustivement à l'article 8. Elles recouvrent notamment les données à caractère personnel ayant pour objet les litiges soumis aux cours, tribunaux et juridictions administratives ou les infractions dont une personne est soupçonnée ou dans lesquelles elle est impliquée. On retrouve en matière de données judiciaires les mêmes principes qu'à l'article 6. Les données ne peuvent être traitées qu'aux fins déterminées par ou en vertu de la loi et des conditions particulières à leur traitement peuvent être prévues par arrêté royal.

L'article 8, § 5, tempère toutefois le principe d'interdiction du traitement des données judiciaires hors intervention du législateur. Le Roi peut autoriser ce traitement, si avis préalable en est donné à l'intéressé, moyennant le respect des conditions restrictives énumérées à la même disposition (108). Cette habilitation don-

(97) Et le cas échéant notifiée dans la déclaration préalable à déposer auprès de la Commission de protection de la vie privée.

(98) Voy. dans le même sens l'avis 10/92 du 20 août 1992 de la Commission de protection de la vie privée, *op. cit.*, p. 122.

(99) Bien que la loi n'exige pas explicitement que les traitements du secteur public soient mis en place sur base de lois (cf. *supra*), l'application du principe général de légalité (toute mission confiée au secteur public doit être définie au sein d'une loi) permet tout de même d'établir que les traitements publics doivent trouver leur fondement dans une loi.

(100) Th. Léonard et Y. Poullet, *op. cit.*, pp. 260 et s.

(101) Cette règle n'est pas énoncée explicitement dans la loi mais elle découle de l'application stricte du principe de finalité.

(102) Article 9 concernant le devoir d'information des personnes fichées lors du premier enregistrement.

(103) Voy. par ex. S. Simitis, « Les données sensibles en quête d'un régime juridique », *Problèmes législatifs de la protection des données*, Athènes, 18-20 nov. 1987, Conseil de l'Europe, ministère de la Justice de Grèce, Athènes, Ant. N. Sakkoulas, 1991, pp. 286-300.

(104) La Convention du Conseil de l'Europe (art. 6) et la proposition de directive communautaire (art. 8) envisagent également la problématique des données sensibles de manière isolée. La plupart des législations nationales adoptent la même approche.

(105) Les listes « exhaustives » de données dites « sensibles » diffèrent sensiblement d'un pays à l'autre.

(106) Article 6, al. 1er, de la loi. Les mots « par ou en vertu de la loi » recouvrent deux possibilités. Soit le législateur déterminera explicitement les finalités légitimes de traitement, soit, par une loi particulière il habilitera le Roi à réglementer cette question. A ce propos, le Conseil d'Etat a fait remarquer qu'il n'est pas opportun que des délégations soient accordées au Roi par les mots « en vertu » puisque la protection de la vie privée relève du domaine des droits et des libertés fondamentales (*Doc. parl.*, Ch. repr., sess. ord. 1990-91, n° 1610/1, p. 54). Le second alinéa de cet article requiert, en outre, l'avis préalable de la Commission de la vie privée.

(107) Article 6, al. 4. L'arrêté doit être délibéré en conseil des ministres et l'avis de la Commission de la vie privée est requis.

(108) Le paragraphe 5 de l'article 8, précise que l'avis donné à l'intéressé doit être *écrit* et que le traitement ne peut être opéré que par des personnes physiques ou morales de droit public ou de droit privé, désignées par arrêtés royaux délibérés en Con-

née au Roi affaiblit dans une mesure certaine la portée de l'interdiction énoncée au premier paragraphe de l'article 8. Il est d'ailleurs peu aisé de comprendre la volonté du législateur lorsqu'il pose en principe la nécessité d'une loi pour déterminer les finalités légitimes de traitement et dans le même temps prévoit une procédure d'exception par arrêté royal qui recouvre largement le champ d'application du principe. Le législateur a, par ailleurs, organisé de multiples exceptions pour lesquelles le traitement des données judiciaires est permis (109).

2.2.2. — *Les données médicales*

55. — L'article 7 de la loi, quant à lui, met sur pied un régime de protection spécifique aux données médicales (110). Ces dernières sont définies de manière générique. Elles englobent les « données à caractère personnel dont on peut déduire une information sur l'état antérieur, actuel ou futur de la santé physique ou psychique, à l'exception des données purement administratives ou comptables relatives aux traitements ou aux soins médicaux ». La possibilité de déduire d'une donnée une information sur l'état de santé d'un individu demeure bien entendu une simple question d'interprétation. Cette approche strictement descriptive est, en réalité, empruntée à la loi sur la Banque-carrefour de la sécurité sociale. Aux termes du premier rapport d'activité du comité de surveillance de la Banque-carrefour, la spécificité de la notion de donnée médicale tient essentiellement au fait que sa connaissance, sa détention et sa communication « nécessitent l'intervention d'un médecin ». Les informations couvertes par le secret médical sont ici clairement visées, bien que ce critère ne soit pas limitatif en soi (111).

Le traitement des données médicales n'est autorisé que *sous la surveillance et la responsabilité d'un praticien de l'art de guérir* (112). Une exception substantielle est toutefois prévue dans la mesure où l'intéressé fait connaître *par écrit son consentement « spécial »* au traitement des données médicales qui lui sont propres (113). Des garanties additionnelles sont encore envisagées. Ainsi, le responsable du traitement (114) doit désigner nominativement les personnes habilitées à intervenir dans le traitement de ces données et à y accéder ainsi que les modalités d'accès au traitement (115). Le texte fait ici référence aux personnes qui interviennent activement dans le traitement des données, tels le médecin, l'infirmière, ... (116).

56. — *La communication des données médicales* fait également l'objet de restrictions (117). En principe, toute communication est interdite sauf si la *loi* en dispose autrement (118). La loi évoque par ailleurs la théorie du secret partagé (119) en autorisant la communication entre praticiens de l'art de guérir (et à leur équipe médicale) en cas *d'urgence médicale* (120). A défaut, *l'intéressé peut également y consentir par écrit* (121). Il nous semble que ce consentement doit être envisagé isolément et, à tout le moins, qu'il ne peut être déduit à titre implicite du consentement au traitement.

Le consentement de l'individu, quasiment absent du texte de la nouvelle loi, reçoit une place particulière en ce qui concerne le traitement et la communication des données médicales. Il semble que ce consentement doit être compris comme une garantie renforçant l'exigence générale de respect du principe de finalité lors du traitement de ces données. En tout état de cause, il reste obligatoire que le traitement ou la communication de données médicales s'inscrive dans une finalité légitime et déterminée et que les données utilisées se limitent aux données nécessaires à l'accomplissement de cette finalité (122).

Enfin, *l'accès de l'intéressé aux données médicales le concernant* doit se faire par l'intermédiaire d'un médecin (123). Faut-il dès lors considérer que le médecin doit se cantonner à un

seil des ministres, après avis de la Commission de la protection de la vie privée. Sur cette question, le professeur Rigaux doute qu'un avis préalable donné par écrit à l'intéressé constitue une garantie appropriée au sens de l'article 6 la Convention du Conseil de l'Europe du 28 janvier 1981 (F. Rigaux, « La protection de la vie privée à l'égard des données à caractère personnel », *op. cit.*, p. 67).

(109) Le législateur a prévu avec logique que ces données judiciaires peuvent être traitées sous la surveillance et la responsabilité d'un avocat, dès lors qu'elles concernent les besoins de la défense des intérêts de ses clients et pour autant que l'accès en soit réservé à l'avocat lui-même, à ses collaborateurs ou aux personnes qui seraient amenées à le remplacer dans l'exercice de ses fonctions (art. 8, § 6, de la loi). Plus spécifiquement encore, le législateur a prévu diverses dérogations qui s'appliquent uniquement à certaines catégories de données judiciaires. Nous nous permettons de renvoyer le lecteur au texte législatif pour plus de détails. Notons seulement que les données portant sur les litiges soumis aux cours, tribunaux et juridictions administratives peuvent être traitées par des personnes physiques ou morales de droit public ou de droit privé uniquement aux fins de gestion de leur propre contentieux (art. 8, § 3). Le traitement de certaines données par le casier judiciaire central est également autorisé. Les casiers judiciaires communaux bénéficient d'une même latitude, bien qu'elle n'ait pas nécessairement trait aux mêmes données (art. 8, § 4). Voy. l'avis critique du Conseil d'Etat sur les notions de casier judiciaire qui ne répondent à aucune dénomination officielle et n'ont aucune existence légale (*Doc. parl.*, Ch. repr., sess. ord. 1990-1991, n° 1610/1, p. 55).

(110) L'évolution de la médecine a conduit à une informatisation généralisée du secteur médical. Dès lors, même si le terme « dossier médical » est largement utilisé dans ce secteur, il s'agit la plupart du temps de traitements et non de dossiers au sens de la loi.

(111) Ainsi, sont assurément des données médicales à caractère personnel, les données reprises généralement dans le dossier médical proprement dit, mais aussi les demandes de remboursement de services et de prestations médicales. Par contre, la résidence d'une personne, son sexe, la seule constatation de l'existence d'un dossier personnel auprès d'un organisme d'exécution de la sécurité sociale ne doivent pas être considérés comme telles (voy. le premier rapport d'activité du comité de surveillance près de la Banque-carrefour de la sécurité sociale, *Rapport d'activité 1992*, Bruxelles, 1992, p. 35).

(112) L'expression « praticien de l'art de guérir » a été substituée au terme de médecin présent dans le texte initial. D'autres professionnels de la santé tels les dentistes et les pharmaciens sont dès lors obligés de la même manière (voy. l'article 1er de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'art de guérir, à l'exercice des professions qui s'y rattachent et aux commissions médicales, *M.B.*, 14 novembre 1967, err. 12 juin 1958).

(113) Le ministre de la Justice a précisé que le consentement « spécial » donné par écrit ne doit pas être obtenu pour chaque acte individuellement (Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, 413/12, p. 93). Il ne faut pas non plus comprendre ce consentement comme ayant une portée illimitée. Sur cette question, le conseil national de l'Ordre des médecins s'était étonné que le consentement de l'individu puisse autoriser le traitement des données médicales, ce qui offrirait moins de garanties puisque le traitement serait opéré hors de la surveillance et de la responsabilité d'un médecin (note du bureau du conseil national de l'Ordre des médecins concernant l'article 8 du projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, annexe 3 au rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, n° 413/12, p. 106).

(114) Par responsable du traitement, il faut entendre le praticien de l'art de guérir sous la responsabilité duquel s'opère le traitement et qui n'est pas nécessairement le maître du fichier, voy. Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445-2, p. 53. En cas de non respect des prescriptions légales, déterminer la personne pénalement responsable risque de donner lieu à quelque difficulté lorsque praticien de l'art de guérir, responsable du traitement des données médicales, et maître du fichier ne seront pas une seule et même personne.

(115) Le contenu et l'étendue de l'autorisation d'accès doivent être précisés pour chaque personne autorisée. Le tout doit être consigné dans un registre régulièrement mis à jour.

(116) Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445-2, p. 91.

(117) Article 7, al. 4, de la loi.

(118) Dans ce cas, l'avis préalable de la Commission de la vie privée est nécessaire. L'exception légale au principe de communication des données médicales est conforme à la réglementation en vigueur relative au secret professionnel. En effet, l'article 458 du Code pénal ne punit pas la révélation du secret lorsque la loi impose celle-ci.

(119) P. Lambert, *Le secret professionnel*, Bruxelles, Némésis, 1985, pp. 121 et s.

(120) Les conditions auxquelles est soumise la communication des données médicales entre praticiens sont donc particulièrement restrictives si on les compare à ce qui prévaut actuellement. Voy. notamment P. Lambert, *op. cit.*, p. 158 et l'article 13 de l'arrêté royal n° 78 relatif à l'art de guérir.

(121) La loi exige une fois de plus un consentement *spécial*. L'ordre des médecins s'insurge contre le consentement du patient qui autoriserait la transmission à un médecin intervenant pour un tiers comme, par exemple, l'employeur du patient. Il s'appuie sur l'article 129 du Code de déontologie médicale qui dispose que le médecin traitant est tenu au secret médical même à l'égard des médecins contrôleurs, des médecins-conseil, des experts-médecins... L'autorisation du patient ne suffit pas à relever le médecin de son secret professionnel (note du bureau du conseil national de l'Ordre des médecins, annexe 3 au rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. extr. 1991-1992, n° 413/12, p. 108).

(122) L'article 7 tend à organiser un régime particulièrement protecteur à l'égard des données médicales. Ces deux exigences doivent dès lors être comprises comme se complétant en vue de renforcer la protection accordée à l'individu.

(123) La communication des données médicales à l'intéressé est organisée à l'article 10, § 3, de la loi.

rôle d'intermédiaire pour rendre les informations compréhensibles au patient, ou qu'il demeure juge de l'opportunité de communiquer les données ? Interpréter la loi comme autorisant le patient à exiger du médecin qu'il l'informe de toute donnée médicale pourrait conduire à remettre en question le système d'information du patient tel qu'il existe actuellement (124).

Par ailleurs, le droit d'accès s'étend à toutes les données médicales reprises dans un traitement. Un individu pourrait-il dès lors s'adresser à son médecin de famille pour lui demander d'exercer son droit d'accès à l'égard des données médicales détenues à son sujet par la compagnie d'assurances dont il est le client ? En effet, la loi précise que les données médicales sont communiquées à l'intéressé par l'intermédiaire d'un médecin *choisi par lui*. Dans cet exemple, il pourrait donc s'adresser à son médecin de famille plutôt qu'au médecin conseil de la compagnie d'assurances.

2.2.3. — *Remarques finales*

57. — Les systèmes instaurés pour les données médicales et judiciaires sont relativement détaillés et prennent des options distinctes des principes actuellement en vigueur. Il nous semble qu'un règlement décisif de ces questions ne trouve pas sa place dans une loi qui a pour vocation de réglementer de manière générale le traitement des données à caractère personnel. S'il est clair que tant les données judiciaires que les données médicales en font partie, les questions de la licéité de leur traitement et surtout de leur communication auraient rendu nécessaire à elles seules un débat spécifique.

58. — Au terme de l'examen du régime mis en place en matière de données sensibles (125), il nous semble que le choix opéré par le législateur d'envisager cette question à titre spécifique n'est pas à l'abri de toute critique. Certes, le législateur semble être conscient du fait qu'une donnée n'est pas sensible *en soi*. Le régime restrictif instauré ne se fonde pas sur l'idée que le traitement de certaines données doit être réservé car celles-ci font partie d'un « noyau dur de la vie privée ». Le législateur a plutôt voulu prévenir tout risque de discrimination *a priori* basée sur ces données. Ainsi, des données relatives à l'origine raciale sont susceptibles de servir de fondement à des pratiques discriminatoires. Pareille motivation nous paraît légitime mais fallait-il pour autant instituer un régime aussi restrictif ? Le caractère sensible ou ordinaire d'une donnée ne doit pas s'apprécier dans l'absolu, mais bien davantage à la lumière de son contexte spécifique d'utilisation (126). Il nous paraît, dès lors, qu'une application correcte et nuancée du principe de finalité légitime offre une protection adéquate (127). Une garantie supplémentaire aurait pu consister à recueillir le consentement libre et éclairé de l'individu pour traiter des données sensibles.

3. — LES DROITS ET LES OBLIGATIONS

59. — Ayant posé les principes à la base de la protection de l'individu, le législateur s'est attaché à organiser le contrôle de leur application. Il a ainsi mis en place un réseau de droits et obligations censés assurer au mieux la transposition des principes lors de la mise en place et de la gestion d'un traitement de données.

Le maître du fichier, ou le cas échéant son représentant en Belgique, est généralement désigné comme responsable du respect de ces prescriptions légales. Leur violation peut être sanctionnée pénalement.

60. — Il a paru opportun, pour l'analyse qui suit, de procéder selon l'ordre pratique des questions auxquelles le maître du fichier est confronté lorsqu'il envisage de mettre sur pied et de gérer un traitement de données. La première démarche à effectuer consiste à déclarer le traitement auprès de la Commission de la vie privée. Il faut ensuite informer la personne concernée, soit lors de la collecte des informations, soit lors de leur premier enregistrement. Le maître du fichier doit encore permettre à l'individu d'exercer les droits d'accès et de rectification qui lui sont reconnus par la loi. L'individu dispose enfin d'un droit de recours en justice.

3.1. — Les obligations du maître du fichier

3.1.1. — *La déclaration auprès de la Commission de la protection de la vie privée*

61. — La loi organise une formalité de déclaration du traitement *automatisé* avant sa mise en œuvre proprement dite. Elle entend par là assurer une information claire et complète tant à l'égard de la Commission de la protection de la vie privée, en lui fournissant les informations nécessaires à l'exercice de ses missions de contrôle, que du citoyen qui doit disposer des éléments nécessaires à l'exercice de ses droits (128). A cet effet, les différentes déclarations sont regroupées et consignées dans un registre (129). Ce dernier reprend la liste des traitements automatisés et de leurs principales caractéristiques ainsi que celle des fichiers manuels susceptibles de porter atteinte à la vie privée. C'est dans ce registre accessible au public que le citoyen trouvera l'information préalable à l'exercice efficace de ses droits.

62. — La formalité de déclaration mise explicitement à charge du maître du fichier ne s'applique qu'aux traitements *automatisés* et ne concerne pas les fichiers manuels sauf si la Commission estime, dans des cas particuliers, ces fichiers susceptibles de porter atteinte à la vie privée (130). Une procédure d'exemption ou de déclaration simplifiée est envisageable pour les traitements automatisés ne présentant clairement pas de risque d'atteinte à la vie privée (131). Contrairement au système français où la C.N.I.L. a la compétence d'édicter des normes simplifiées, la solution belge requiert l'intervention du Roi (132). On peut se demander pourquoi ce rôle n'a pas été dévolu à la Commission dont les membres sont spécialement compétents pour juger de l'opportunité et de l'ampleur de la déclaration à effectuer. Une telle approche aurait contribué à alléger un système administratif particulièrement lourd.

63. — La déclaration comporte une description des caractéristiques du traitement. Il s'agit essentiellement de l'identification du maître du fichier, du but poursuivi, de sa description et des catégories de personnes admises à obtenir les données (133). Deux situations donneront lieu à un complément de déclaration. D'une part, lorsque la Commission de la protection de la vie privée effectue une démarche à cet effet (134) et, d'autre part, lorsque les données traitées sont destinées à être transmises *vers*

(124) Sur la question de savoir dans quelle mesure le secret médical peut être opposé au patient, la doctrine n'est pas unanime. A ce sujet, voy. P. Lambert, *op. cit.*, pp. 115-117, D. Thouvenin, *Le secret médical et l'information du médecin*, Lyon, Presses universitaires de Lyon, 1982, pp. 58 et s. et R.O. Dalcq, « Réflexions sur le secret professionnel », *R.G.A.R.*, 1986, p. 11053. Quant à la déontologie médicale, elle admet des restrictions au principe de révélation du diagnostic au patient (art. 33, C. de déontologie).

(125) Rappelons que désireux de préserver toute l'efficacité des régimes de protection mis en place, le législateur a érigé en principe l'interdiction de collecter en Belgique des données sensibles destinées à être traitées à l'étranger (art. 4, § 2, de la loi); voy. *supra*, n° 36.

(126) Dans le même sens, voy. S. Simitis, *op. cit.*, pp. 286-300; P. et Y. Poullet « 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, C.I.E.A.U.-C.R.E.A.D.I.F., pp. 25 et s.

(127) Appliquer le principe de finalité aurait permis d'éviter de devoir multiplier les exceptions chaque fois que le traitement de données sensibles est légitime.

(128) Article 17 de la loi qui détaille notamment les mentions de la déclaration. La formalité de déclaration s'accompagne du paiement d'une redevance, ce qui est contraire à l'option retenue dans la majorité des pays européens (art. 17, § 9, de la loi). Les modalités de règlement de la redevance seront précisées par arrêté royal en fonction du type de déclaration et de l'importance du traitement déclaré. La loi précise cependant que le montant de la redevance ne pourra excéder 10.000 F. Le Conseil d'Etat se montre critique à l'égard de cette 'redevance' estimant qu'il s'agit en réalité d'un impôt et qu'il appartient au législateur d'en fixer l'assiette et le taux (voy. avis du Conseil d'Etat, *Doc. parl.*, Ch. repr., sess. ord., 1990-1991, 1610/1, p. 60).

(129) Article 18. Seules les indications reprises à l'article 17, §§ 3 et 6, sont visées.

(130) Article 19. Cet article fonde le pouvoir d'intervention de la Commission à l'égard des fichiers manuels.

(131) Article 17, § 8.

(132) Le Roi agit sur proposition ou avis de la Commission. L'avis donné par celle-ci ne doit pas être conforme.

(133) Le détail des mentions est repris à l'article 17, § 3, de la loi.

(134) Article 17, § 4. Le complément de déclaration portera en particulier sur l'origine des données, la technique d'automatisation choisie et les mesures de sécurité prévues.

l'étranger (135). Si le traitement venait à être supprimé ou si une des mentions de la déclaration devait être modifiée, une notification ou nouvelle déclaration est requise (136). Nul doute qu'il en sera ainsi lorsque les données seront traitées en vue d'une finalité différente de celle prévue dans la première déclaration.

64. — La formalité de déclaration suscite de vives critiques au sein des milieux concernés (137). Les maîtres de fichiers y voient la source de charges importantes. La Commission elle-même craint d'être paralysée par d'écrasantes tâches administratives qui la détourneraient de missions plus essentielles (138). A ses yeux, une notification limitée à quelques mentions qui constitueraient les données du registre public serait plus adéquate (139). A ces critiques, il est important d'ajouter que la lourdeur du système de déclaration sera largement fonction de l'interprétation qui sera donnée au concept de traitement automatisé, concept à la base de la formalité de déclaration (une déclaration par traitement) (140). Si l'on admet que le critère unificateur du traitement est la finalité poursuivie par le maître du fichier, il faut encore préciser comment cette finalité doit être appréhendée. Peut-on se contenter d'une approche générique ou à l'autre extrême envisager de manière séparée chaque application poursuivant un but distinct ? Ainsi, une entreprise pourra-t-elle se contenter de déclarer un traitement de « gestion du personnel » ou devra-t-elle répéter cette formalité pour un traitement opéré en vue du paiement des salaires, pour un traitement servant à répartir le personnel dans les locaux, pour un traitement visant à éditer un annuaire téléphonique interne à l'entreprise... ? Le travail délicat qui incombera dans un premier temps à la Commission, consistera à définir les termes d'un juste équilibre entre, d'une part, une définition du traitement suffisamment large pour que la formalité de déclaration puisse être praticable et effective et, d'autre part, une approche trop laxiste qui nuirait à la fonction première de cette exigence, à savoir permettre tant à l'individu qu'à la Commission de connaître et de contrôler les chemins empruntés par l'information à caractère personnel et les buts de son utilisation.

(135) Article 17, § 6. Doivent alors être mentionnées les catégories de données faisant l'objet de la transmission et le pays de destination pour chaque catégorie de données.

(136) Article 17, § 7.

(137) Pour une critique plus générale de l'obligation de déclaration, voy. S. Simitis, *op. cit.*, p. 62.

(138) Pour une critique des formalités préalables à la création des traitements automatisés en France, voy. J. Huet et H. Maisl, *Droit de l'informatique et des télécommunications*, Paris, Litec, 1989, p. 205. En Belgique, pensons seulement au nombre d'inscrits dans le registre de commerce et multiplions ce nombre par les différents traitements à déclarer. Si l'on y ajoute les déclarations effectuées par l'administration et les professions libérales, on imagine sans peine la difficulté qu'aura la Commission à gérer les déclarations.

(139) Voy. l'avis du 12 mai 1992 de la Commission de la protection de la vie privée concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *op. cit.*, p. 94.

(140) Voy. point 1.1.2.1.

3.1.2. — *L'information de la personne concernée*

65. — La volonté d'assurer à l'individu une transparence des circuits informationnels est encore le fondement d'une autre obligation mise à charge du maître du fichier, à savoir l'obligation de renseigner la personne concernée. Cette obligation est remplie lors de la collecte des informations auprès de celle-ci ou lorsque les données sont enregistrées pour la première fois (141).

3.1.2.1. — *L'information lors de la collecte.*

66. — L'article 4 de la loi impose à *quiconque* recueille des données à caractère personnel en vue d'un traitement d'informer la personne concernée par celles-ci (142). Il s'agira généralement du maître du fichier, mais ce pourrait également être une personne recueillant des données pour le compte de celui-ci.

L'objectif recherché est de sensibiliser la personne concernée en la rendant attentive aux éventuels risques d'atteinte à sa vie privée que pourrait occasionner le traitement. Il s'agit également de l'informer des droits spécifiques qui lui sont conférés.

67. — Les informations communiquées à l'individu auprès duquel la collecte est effectuée concernent l'identité du maître du fichier, la base légale ou réglementaire de la collecte des données, la finalité d'utilisation des données, la possibilité de se renseigner auprès du registre public et, enfin, l'existence des droits d'accès et de rectification (143). Le champ d'application territoriale de l'obligation est défini à l'article 4. L'information doit être fournie, en tout état de cause, à partir du moment où la collecte est effectuée sur le territoire belge, sans que le fait que le traitement soit effectué en Belgique ou à l'étranger n'entre en considération (144).

La forme selon laquelle l'information doit être communiquée n'est pas précisée et cela, aux termes de l'exposé des motifs, afin de conserver au mécanisme le maximum de souplesse (145). Il appartiendra à celui qui collecte les informations de déterminer le moyen le plus adéquat de remplir son obligation.

68. — C'est par le biais de cette seule obligation d'information que la loi aborde le problème de la collecte des données. L'article 5 de la Convention du Conseil de l'Europe énonce pourtant le principe de licéité et de loyauté de la collecte. L'importance d'un tel principe aurait dû conduire à le transposer de manière plus complète dans la loi. La loyauté de la collecte renvoie notamment au contexte dans lequel les données sont obtenues, à la légitimité des finalités poursuivies par le traitement et à la pertinence des données collectées par rapport à ces finalités (146). Nulle disposition de la loi ne permet de sanctionner directement un procédé déloyal de collecte qui consisterait par exemple en ce que des informations sur les habitudes de vie d'un individu soient obtenues auprès de son voisin.

3.1.2.2. — *L'information lors du premier enregistrement.*

69. — L'obligation d'informer la personne concernée au moment où elle est enregistrée *pour la première fois dans un traitement déterminé* est prescrite à l'article 9 de la loi (147). Il a déjà été dit que c'est la finalité poursuivie qui permet de distinguer un traitement d'un autre. Dès lors, à partir du moment où le maître du fichier modifie cette finalité, il met en œuvre un nouveau traitement et doit en conséquence en informer la personne concernée. Les renseignements à fournir sont analogues à ceux qui doivent être communiqués lors de la collecte.

70. — Le législateur a assorti cette exigence de maintes exceptions. La première se rapporte aux traitements destinés à l'établissement et à la diffusion de statistiques anonymes (148). D'autres restrictions sont motivées par des impératifs de sécurité (149). Le plus vaste groupe d'exceptions se fonde sur la connaissance préalable que la personne concernée a de l'enregistrement. Il en est ainsi :

— lorsqu'une *information* a été fournie lors de la *collecte*;

— lorsque le traitement se situe dans un *rapport contractuel* noué entre la personne concernée et le maître du fichier (150). Une telle

(141) L'obligation d'information existe indépendemment du fait qu'il s'agisse d'un traitement automatisé ou de la tenue d'un fichier manuel. Voy. exposé des motifs du projet de loi, *Doc. parl.*, Ch. repr., sess. ord. 1990-1991, n° 1610/1, p. 23.

(142) Les sanctions pénales prescrites à l'article 39 punissent quiconque recueille, en vue d'un traitement, des données à caractère personnel sans donner les informations requises.

(143) Pour le contenu précis des informations, voy. l'article 4, § 1er, 1° à 5°. Comme l'expriment dans leurs avis tant le Conseil d'Etat (*op. cit.*, pp. 53-54) que la Commission de la vie privée (avis du 12 mai 1992, *op. cit.*, p. 86), il est regrettable que le caractère obligatoire ou facultatif des réponses ne soit pas mentionné.

(144) Certaines exceptions motivées par des intérêts considérés comme supérieurs sont cependant prévues. Les traitements gérés par des autorités publiques en vue de l'exercice de leurs missions de police judiciaire et administrative ne donnent pas lieu à une obligation d'information (pour le détail voy. l'article 11, 2°, 3° et 4° de la loi).

(145) Exposé des motifs du projet de loi, *Doc. parl.*, Ch. repr., sess. ord., 1990/1991, n° 1610/1, p. 9.

(146) F. Rigaux, *La protection de la vie privée et les autres biens de la personnalité*, Bruxelles, Bruylant, 1990, p. 585, n° 526.

(147) L'article 9 précise que la personne concernée doit être « immédiatement » informée. Le caractère d'immédiateté a suscité des réactions au sein des milieux concernés. Ceux-ci s'interrogent sur la durée du délai dans lequel ils doivent remplir leur obligation.

(148) Article 11, 1°.

(149) Il s'agit des traitements gérés par les autorités publiques en vue de leur mission de police judiciaire et administrative, exception identique à celle reprise en matière d'information lors de la collecte, détaillée à l'article 11.

(150) On peut s'étonner de l'interprétation que les travaux parlementaires donnent de la relation contractuelle. Cette dernière ne doit pas être entendue dans son acception strictement juridique, mais dans un sens plus large. Il suffit que le traitement s'inscrive dans le cadre d'une relation de nature à justifier le traitement. Une telle interprétention élargit consi-

exception paraît peu fondée; la relation contractuelle n'implique pas que l'individu connaisse *a priori* toutes les finalités d'utilisation de ses données poursuivies par son cocontractant. De plus, cette exception peut avoir des conséquences inattendues lorsque des renseignements concernant une personne sont recueillies auprès d'un tiers qui est lui-même en relation contractuelle avec le maître du fichier (151);

— lorsque le traitement est opéré dans le cadre d'une *relation* entre la personne concernée et le maître du fichier, *réglée par ou en vertu d'une loi, d'un décret ou d'une ordonnance* (152).

71. — Indépendamment des exceptions énoncées formellement dans la loi, le législateur a mis en place une procédure particulière d'exemption. Un arrêté royal délibéré en conseil des ministres peut, sur avis de la Commission de la protection de la vie privée, soit soustraire certaines catégories de traitements à l'obligation, soit organiser une procédure d'information collective applicable à certains types de traitement (153). Il s'agira dans ce cas de mettre en balance l'ampleur de l'ouvrage ou les frais démesurés auxquels une information individuelle pourrait donner lieu et le bénéfice pour l'individu qu'une telle information présente.

72. — A ce stade, il est relativement malaisé d'estimer quelle sera la portée du devoir d'information lors du premier enregistrement. Les nombreuses réserves formulées en termes larges et peu rigoureux et la possibilité d'exemption par arrêté royal paraissent effectivement alléger dans une proportion substantielle l'étendue de ce devoir. Plutôt que de partir d'un principe d'information puis d'en réduire considérablement la portée en organisant de nombreuses exceptions, il nous semble que la logique du texte impliquait de ne pas prévoir de formalité d'information hormis dans des cas spécifiques (154).

3.1.3. — *La gestion du traitement*

73. — Une fois le traitement de données mis en place, le maître du fichier aura en outre à le gérer en respectant les obligations énoncées à l'article 16 de la loi. Il devra :

— *établir* pour chaque traitement automatisé *un état* qui mentionnera la nature des données traitées, le but du traitement, les rapprochements, interconnexions et consultations, ainsi que les tiers à qui les données sont transmises. Cet état interne sera extrêmement utile tant à l'entreprise elle-même, amenée à s'interroger sur ses propres pratiques, qu'à la Commission de la protection de la vie privée lors de l'accomplissement de ses missions de contrôle. Rappelons cependant que le traitement automatisé fera déjà l'objet d'une déclaration au contenu similaire auprès de la Commission, déclaration dont la lourdeur administrative a déjà été soulignée;

— vérifier la *conformité des programmes* servant au traitement automatisé *avec les termes de la déclaration* effectuée auprès de la Commission. Il contrôlera également la *régularité de leur application*;

— faire toute diligence pour tenir les données *à jour, rectifier* ou *supprimer* les données inexactes, incomplètes ou non pertinentes. La même obligation s'applique aux données obtenues ou traitées en méconnaissance des articles 4 à 8 (155);

— prendre soin, d'une part, à ce que *l'accès* au traitement ne soit concédé qu'aux personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux informations enregistrées. Il doit veiller à ce que ces personnes ne puissent effectuer des modifications, ajouts, effacements, lectures, rapprochements ou interconnexions non prévus, non autorisés ou interdits. D'autre part, il s'assurera que la communication des données n'ait lieu qu'à destination des seules personnes autorisées.

Le maître du fichier est tenu de faire connaître aux utilisateurs internes des données la teneur de la nouvelle loi ainsi que toute autre prescription relative aux exigences particulière de la vie privée face aux traitements de données à caractère personnel.

Il doit, enfin, adopter les mesures techniques et organisationnelles adéquates en vue de garantir la sécurité des données. Pour la première fois en droit belge, l'obligation d'assurer la sécurité technique de l'information est énoncée. Certes, elle doit se comprendre 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 contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel » (156).

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 et, d'autre part, aux menaces virtuelles et à la nature des données à protéger (157). 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.

74. — 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 » (158).

3.2. — Les droits de la personne concernée

75. — La loi confère à l'individu des droits spécifiques lui permettant en premier lieu d'accéder aux données à caractère personnel le concernant et, le cas échéant, d'en obtenir la rectification (159). De plus, il peut introduire un recours en justice relatif à l'exercice de ces deux droits selon une procédure particulière.

3.2.1. — *Le droit d'accès*

76. — La loi reconnaît à toute personne fichée la faculté de prendre connaissance des données enregistrées à son sujet. Le droit d'accès est le préliminaire obligé pour permettre à la personne concernée d'effectuer son contrôle. L'expérience à l'étranger révèle, cependant, que ce droit individuel ne constitue pas réellement une protection adéquate. Il n'est que très rarement mis en œuvre (160). La raison en est-elle à trouver dans l'inertie qui caractérise le citoyen, dans la mauvaise foi des ficheurs, ou dans la crainte que peut éprouver un individu d'exercer ce droit à l'encontre de son employeur ou d'une administration ?

L'article 10 dispose, en premier lieu, que la mise en œuvre du droit d'accès ne nécessite qu'une demande datée et signée adressée au maître du fichier (161), voire le paiement d'une redevance limitée à la couverture des seuls frais administratifs. Les renseignements doivent être communiqués sans délai et, au plus tard, dans les quarante-cinq jours de la réception de la demande. Quoique le texte ne le stipule pas, il va de soi que la communication des informations doit être fidèle à ce qui est enregistré et

dérablement la portée de l'exception et nous semble contredire le prescrit légal. Par ailleurs, si la relation contractuelle est définitivement terminée et qu'il ne subsiste ni droits ni devoirs, le lien est rompu (*Doc. parl.*, Sén., sess. extr., 1991-1992, n° 445-2, p. 93).

(151) Voy. P. Claes et J. Dumortier, « Bescherming en gegervensverwerking bij het personeelsbeleid », Orientatie, janvier 1993, p. 9.

(152) La portée de cette exemption est difficile à évaluer. Ainsi, les rapport entre l'administration et les citoyens ne sont-ils pas toujours réglementés ?

(153) Article 9, al. 3.

(154) Voy. sur cette question l'avis du 12 mai 1992 de la Commission de la protection de la vie privée, *op. cit.*, p. 90.

(155) Il s'agit de la transposition de l'article 5, d, de la Convention du Conseil de l'Europe qui prescrit que les données doivent être exactes et si nécessaire mises à jour. Cependant, les termes de l'article 5, d, laissent supposer qu'il s'agit d'une obligation de résultat, alors qu'il ne s'agit dans la loi que d'une obligation de moyen.

(156) Article 16, § 3. Cette disposition s'inspire de l'article 17 de la proposition de directive. L'article 7 de la Convention du Conseil de l'Europe contient également une disposition en matière de sécurité.

(157) Des normes appropriées pour toutes ou certaines catégories de traitements pourront être édictées par le Roi sur avis de la Commission de la vie privée.

(158) Exposé des motifs du projet de loi, *op. cit.*, p. 21.

(159) Articles 10 à 13. Les droits d'accès et de rectification concernent de la même manière le traitement automatisé et la tenue d'un fichier manuel (Exposé des motifs du projet de loi, *op. cit.*, pp. 23-24). Notons que la jurisprudence n'a pas attendu la loi pour reconnaître ces droits à la personne fichée; voy. particulièrement Trib. Civ. Liège, 11 mars 1987, *J.L.M.B.*, pp. 549 à 560 et Liège, (3e ch.), 5 juin 1991, *J.T.*, 1992, p. 36.

(160) Voy. J. Frayssinet, *op. cit.*, p. 81; F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, *op. cit.*, p. 595, n° 536.

(161) Le Roi peut désigner une autre personne que le maître du fichier à qui il faut s'adresser pour obtenir communication des données.

qu'elle doit être effectuée sous une forme compréhensible pour la personne fichée.

Lors de l'exercice de son droit d'accès, l'individu est averti de son droit d'obtenir la correction des données erronées et de la faculté qui lui appartient d'intenter un recours en justice. Il est aussi « éventuellement » avisé de la possibilité de consulter le registre public tenu auprès de la Commission de la protection de la vie privée (162).

77. — En vue de prévenir d'éventuels abus liés à l'exercice du droit d'accès, le législateur a prévu qu'un délai de douze mois doit s'écouler entre deux mises en œuvre de celui-ci par une même personne (163). Le même intervalle de douze mois doit être respecté à partir du moment où les données ont été communiquées d'office (164).

78. — Dans différentes hypothèses, le législateur, s'inspirant du modèle français, ne laisse pas l'individu accéder directement aux informations le concernant (165). Les données médicales, on l'a vu, sont divulguées à l'intéressé par l'intermédiaire du médecin de son choix (166). La médiation du médecin ne s'applique qu'aux seules données médicales et ne s'étend pas aux données administratives ou comptables.

Des impératifs propres à la sécurité publique requièrent que d'autres données soient soustraites à l'accès direct de l'individu (167). Ces informations peuvent cependant faire l'objet d'« un accès indirect » par l'entremise de la Commission. Cette dernière, après avoir fait procéder aux investigations utiles, se limitera à signifier à la personne concernée que les vérifications ont été effectuées, sans lui livrer le contenu des informations (168).

Dans les deux cas évoqués, un tiers, soit le médecin, soit la Commission de la protection de la vie privée, intervient en tant qu'intermédiaire entre l'individu et les données. Lorsque la Commission joue le rôle de médiateur, il n'est cependant pas question d'un véritable droit d'accès, puisqu'il n'y a pas communication des données à la personne concernée.

La troisième restriction au droit d'accès se rapporte aux données statistiques. Ces dernières ne peuvent faire l'objet d'un droit d'accès que pour autant qu'elles ne soient pas encore rendues anonymes (169). Il ne s'agit pas d'une réelle exception dans la mesure où les données ont perdu leur caractère personnel. Par défaut d'objet, le droit d'accès ne peut nécessairement plus s'exercer.

3.2.2. — *Le droit de rectification*

79. — Du droit d'accès dérive naturellement le droit de rectification. En ce sens, la loi dispose que toute personne fichée jouit du droit d'obtenir gratuitement la rectification d'une donnée *inexacte* qui la concerne (170). De la même manière, elle est en droit d'exiger la *suppression* ou *l'interdiction d'utilisation* de toute donnée qui, compte tenu du *but du traitement*, est *incomplète* ou *non pertinente* ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été *conservée au-delà de la période autorisée* (171). Soulignons que le droit de rectification n'autorise pas cependant la personne concernée à exiger du maître du fichier qu'il supprime de son traitement les données à caractère personnel la concernant. Elle ne peut y prétendre que si les données sont non pertinentes eu égard à la finalité du traitement.

80. — Dans le prolongement du droit de rectification, la loi impose au maître du fichier une obligation complémentaire. Dès réception de la demande tendant à faire rectifier, supprimer ou interdire d'utiliser ou de divulguer des données à caractère personnel ou dès l'introduction d'une action en justice (172), le maître du fichier doit, lorsqu'il communique les données, signifier clairement l'existence d'une contestation (173). Les deux situations mentionnées ne sont pas identiques. Le premier cas vise la seule démarche tendant à obtenir la rectification des données auprès du maître du fichier, tandis que le second vise l'introduction d'une action en justice après un refus de rectification.

Concrètement, à partir du moment où une donnée est contestée, le maître du fichier doit lui adjoindre un indice de doute signalant aux tiers qu'un contrôle est réalisé sur la donnée dont ils prennent connaissance.

81. — Le maître du fichier est enfin tenu de transmettre les rectifications ou suppressions de données aux tiers à qui celles-ci ont été communiquées (174). Afin de conserver tout son sens à cette obligation (175), le législateur précise que le maître du fichier ne doit s'y soumettre que pour autant qu'il connaisse encore les destinataires de l'information. Attentif, malgré tout, à ce que cette exigence ne reste pas lettre morte, il enjoint le maître du fichier de conserver douze mois l'identité des destinataires.

3.2.3. — *Le droit de recours*

82. — La loi organise un recours en faveur de la personne concernée auprès du Président du tribunal de première instance siégeant comme en référé (176). Elle rend ce dernier compétent pour connaître de toute demande relative à l'exercice des droit d'accès et de rectification. L'action n'est recevable que si une demande de droit d'accès ou de rectification a été rejetée ou qu'il n'y a pas été donné suite (177).

L'ordonnance rendue par le tribunal est prononcée en audience publique et est exécutoire par provision nonobstant opposition ou appel.

3.3. — **Remarques finales**

83. — Cet examen des droits et obligations montre que le législateur belge n'a pas fait œuvre originale. S'inspirant largement de la loi française, il a malheureusement négligé de reprendre une disposition particulièrement intéressante de cette loi. Cette dernière reconnaît en effet à l'individu le droit de ne pas être soumis à une décision prise sur le seul fondement d'un traitement qui définit un profil de personnalité (178). L'occasion était pourtant belle de réaffirmer que dans la relation informatique-individu, la personne ne peut être réduite aux conclusions d'une machine. Par ailleurs, il nous semble qu'un autre droit eût trouvé sa place dans la nouvelle loi : le droit de l'individu de s'opposer pour des raisons légitimes à ce que des données le concernant fassent l'objet d'un traitement. Affirmer un tel droit aurait donné la possibilité à la personne concernée de refuser le traitement de ses données (179). Pour ce faire, celle-ci aurait pu invoquer un intérêt légitime, même individuel, supérieur à celui du maître du fichier.

(162) Rappelons à ce propos que la déclaration effectuée auprès de la Commission de la vie privée doit mentionner le service auprès duquel s'exercera le droit d'accès et les mesures prises pour en faciliter l'exercice (art. 17, § 3, 9°).

(163) Article 10, § 2, de la loi. Le délai prend cours à partir de la date de la première demande à laquelle il a été répondu.

(164) Ce délai peut être réduit par la Commission de la protection de la vie privée qui ne peut toutefois intervenir que dans des cas exceptionnels ou lorsqu'une modification des données a eu lieu (art. 10, al. 2, de la loi).

(165) Article 11 de la loi. En France, le droit d'accès indirect est réglé aux articles 39 et 40 de la loi informatique et libertés.

(166) Article 10, § 3, voy. *supra*, n° 56.

(167) Article 13. Il s'agit des données visées à l'article 11, 2° à 4°, à savoir celles reprises dans les traitements gérés par des autorités publiques en vue de l'exercice de leurs missions de police administrative et judiciaire, ainsi que les traitements gérés par la Sûreté de l'Etat, le Service général du renseignement et de la sécurité du ministère de la Défense nationale.

(168) Les modalités de l'accès indirect seront réglées par arrêté royal délibéré en Conseil des ministres sur avis de la Commission (art. 13, al 2 et 3); voy. sur cette question F. Rigaux, « La protection de la vie privée à l'égard des données à caractère personnel », *op. cit.*, pp. 60-61.

(169) Article 11, 1°. Pareille restriction est prévue à l'article 9-3 de la Convention du Conseil de l'Europe.

(170) Article 12, § 1er.

(171) Article 12, § 1er, al. 2. La procédure prévoit que l'intéressé qui souhaite exercer son droit de rectification adresse à cet effet une demande datée et signée au maître du fichier ou à tout autre personne désignée par le Roi.

(172) L'obligation existe tant que la décision n'a pas été coulée en force de chose jugée.

(173) Article 15.

(174) Article 12, § 3.

(175) La possibilité d'exempter certaines catégories de traitement par arrêté royal délibéré en Conseil des ministres après avis de la Commission est prévue et les traitements « de police » sont exclus du champ d'application de cette disposition.

(176) Article 14 de la loi qui détaille la compétence du tribunal, le contenu de la requête, les conditions de recevabilité de la demande, les pouvoirs particuliers du président du tribunal de premère instance, etc.

(177) Article 14, § 5. On peut se demander s'il n'existe pas une contradiction entre l'instauration d'une procédure particulière motivée par l'urgence et le délai d'attente de 45 jours imposé au justiciable avant de pouvoir déclancher cette procédure; voy. en ce sens, l'avis de la Commission de la protection de la vie privée du 12 mai 1992, *op. cit.*, p. 91.

(178) Article 2 de la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La proposition de directive européenne reconnaît ce droit en son article 16, § 1er.

(179) La proposition de directive européenne consacre le « droit d'opposition » en son article 15.

4. — LA COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

4.1. — Introduction

84. — En se dotant d'une législation de protection de la vie privée, la plupart des pays ont dans le même mouvement mis sur pied un organe de contrôle, chargé de veiller à l'application des réglementations édictées (180). Cet organe est envisagé comme un moyen de protéger les libertés du citoyen menacées par le développement de la technologie informatique. Il jouit de compétences variables et sa composition comme ses modes de fonctionnement présentent des caractéristiques diverses : commissions munies de compétences décisionnelles, commissaire, commission « de sages », ... D'ordinaire, ces institutions rassemblent des spécialistes (informaticiens, magistrats, ...) et jouissent d'une large autonomie à l'égard des pouvoirs en place (181).

85. — Certains commentateurs remettent en cause cette indépendance. Les uns en contestent la légitimité, estimant qu'elle constitue une « perversion insensible de la démocratie » exprimant l'abdication de pouvoirs plus légitimement fondés à agir. Ils craignent en particulier que la logique de l'appareil étatique ne soit mise en cause et évoquent par ailleurs un gouvernement des sages voire une dérive aristocratique (182). En effet, l'intervention de ce type d'organe ne bénéficie ni de la légitimité constitutionnelle du juge indépendant, ni de celle d'un parlement souverain élu au suffrage universel, ni de la légitimité de l'administration classique, subordonnée au gouvernement en place (183). D'autres mettent en doute la réalité de l'indépendance. Ils se demandent si cet organe ne serait pas un reflet des pouvoirs en place et ne servirait pas les intérêts de ces derniers, plutôt que ceux des individus (184).

A l'image d'autres pays, la Belgique a également mis sur pied une commission indépendante, garante de la nouvelle réglementation. En réalité, cette commission instituée auprès du ministère de la Justice est déjà en fonction depuis le 1er janvier 1992 (185). Néanmoins, faute d'une réglementation générale, ses attributions restaient limitées à certains secteurs (186). L'adoption de la loi permet donc de lui assigner une mission globale de protection de la vie privée à l'égard des traitements de données à caractère personnel.

4.2. — La composition

86. — La composition de la Commission entend faire la démonstration de son indépendance (187). Il nous paraît dès lors utile de l'examiner. La désignation des membres se fait de deux manières. Une partie des ceux-ci, *les membres de droit*, est choisie par les comités de surveillance institués par les réglementations sectorielles (188). Quant aux autres membres, ils sont nommés directement par le Parlement (tantôt par la Chambre des représentants tantôt par le Sénat) sur base de listes proposées par le Conseil des ministres et comprenant deux candidats pour chaque mandat à pourvoir (189). Pour chacun des mandats sont choisis un membre effectif et un membre suppléant (190). En principe, et les membres effectifs et les membres suppléants seront au nombre de huit. Ce nombre peut être augmenté, les membres de droit ne pourront toutefois jamais être majoritaires au sein de la Commission. Le choix s'est ainsi porté sur une Commission regroupant un nombre important de membres — généralement occupés à temps partiel — plutôt que sur un organe aux effectifs plus réduits mais s'y consacrant à temps plein.

La loi ajoute encore que la Commission devrait être *représentative des différents groupes socio-économiques* (191) et respecter la parité linguistique (192). Elle doit compter au moins un juriste, un informaticien, une personne relevant du secteur public, expérimentée dans les questions de protection des données et une personne disposant des mêmes compétences mais appartenant au secteur privé (193). Quant au président, il doit faire partie des membres désignés par le Parlement et être magistrat. Les membres doivent être experts en matière de système d'information et présenter toutes les garanties pour accomplir leur tâche en toute indépendance. Il nous semble que cette composition pluraliste, si elle existe réellement, facilite l'expression de multiples points de vue mais risque de rendre plus difficile l'adoption de positions communes.

Des conditions liées à l'exercice du mandat visent également à assurer l'indépendance de la Commission. Ainsi, si les membres peuvent être relevés de leur charge par la Chambre qui les a nommés en cas de manquement à leurs devoirs ou d'atteinte à la dignité de leur fonction, ce ne peut en aucun cas l'être à l'occasion des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions (194). Dans les limites de leurs attributions, ils ne sont donc pas soumis au principe de subordination ou de hiérarchie. Ceci différencie sensiblement la Commission d'un organe administratif traditionnel (195). Par ailleurs, les membres sont tenus d'une obligation de confidentialité à l'égard des faits, actes ou renseignements dont ils ont connaissance en raison de leurs fonctions (196).

87. — La Commission est rattachée organiquement au ministère de la Justice, ce qui nous paraît plutôt aller à l'encontre de son indépendance (197). Le ministère en supporte les frais de fonctionnement (personnel, secrétariat, ...). La Commission devrait pourtant disposer d'une certaine autonomie financière puisque le montant des redevances perçues lors de l'accomplissement de la formalité de déclaration est

(180) En guise d'illustration citons en France, la C.N.I.L., aux Pays-Bas, la Registratiekamer, au Canada, le Commissaire à la protection de la vie privée et, au Québec, la Commission d'accès à l'information.

(181) Les institutions sont généralement distinctes de l'administration générale. En France, la loi du 8 janvier 1978 relative à l'informatique, aux fichiers et aux libertés énonce explicitement dans son article 8, 1er, que la Commission nationale de l'informatique et des libertés est une autorité administrative indépendante.

(182) Voy. notamment en France la réflexion de S. Hubac et E. Pisier, « Les autorités face aux pouvoirs », *in* C.A. Colliard et G. Timsit (éd.), *Les autorités administratives indépendantes*, Vendôme, P.U.F., 1988, p. 123.

(183) Voy. également en France sur la difficulté de qualification des autorités administratives indépendantes J. Chevalier, « Réflexions sur l'institution des autorités administratives indépendantes », *J.C.P.*, 1986, I, 3254.

(184) Voy. C. Teitgen-Colly, « Les autorités administratives indépendantes : histoire d'une institution », *in Les autorités administratives indépendantes, op. cit.*, p. 71; P. Sabourin, « Les autorités administratives indépendantes dans l'Etat », *in Les autorités administratives indépendantes, op. cit.*, pp. 111 et s. Cette position est évoquée par A. Vitalis et R. Laperrier, *in* « La démocratie assistée par des sages, l'exemple du contrôle de l'informatisation », colloque A.C.F.A.S., Association canadienne de sociologues et anthropologues de langue française, *Droits-Liberté-Démocratie*, Université du Québec à Montréal, 15-19 mai 1989, pp. 4-5.

(185) La Commission est entrée en fonction sur base de l'article 92 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (*M.B.*, 22 févr. 1990, errata, *M.B.*, 2 juin 1990 et 2 oct. 1990) et de l'arrêté royal du 8 août 1991 réglant la composition et le fonctionnement de la Commission (*M.B.*, 1er oct. 1991), modifié par l'arrêté royal du 17 octobre 1991 (*M.B.*, 24 oct. 1991). Jusqu'au 31 décembre 1991, il existait en Belgique un Commission *consultative* pour la protection de la vie privée compétente, pour certains domaines particuliers du secteur public.

(186) Voy. *supra*, n° 89.

(187) La composition et le fonctionnement de la Commission ont été réglés par l'arrêté royal du 8 août 1991. Cet arrêté royal donnait exécution à l'article 92 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale. Il était cependant largement inspiré de ce qui n'était encore que le projet Wathelet. Les dispositions de cet arrêté royal et de la nouvelle loi présentent donc de fortes similitudes.

(188) Ainsi, la loi instituant la Banque-carrefour de la sécurité sociale a mis sur pied un comité de surveillance chargé de veiller au respect de la loi en vue de la protection de la vie privée. Plus précisément, ce comité vérifie que les communications de données se font conformément aux dispositions légales et que les mesures de sécurité prévues sont bien observées. La création d'un deuxième comité de surveillance est prévue conformément à l'article 72 de la loi relative au crédit à la consommation (*M.B.*, 9 juill. 1991).

(189) Article 23, al. 1er et 24, § 3.

(190) Article 24, § 1er. La durée du mandat est de six ans (art. 24, § 3).

(191) Article 24, § 3, al. 3.

(192) Article 24, § 2.

(193) Article 24, § 3, al. 4.

(194) Article 24, §§ 3 et 5.

(195) Voy. C.A. Collard et G. Timsit, *Les autorités administratives indépendantes*, P.U.F., 1988, p. 11.

(196) Article 33 de la loi. D'autres conditions (être belge, jouir de ses droits civils et politiques et ne pas être membre du Parlement européen, ni du Parlement national ni d'un Conseil de Communauté ou d'un conseil régional) sont également prévues à l'article 24, § 4.

(197) Articles 34-35.

affecté à un fonds assurant son fonctionnement (198).

88. — Les possibilités de la Commission ne doivent pas être surestimées. Les ressources mises à sa disposition restent modestes. Quand au fonds alimenté par les redevances, il sera fonction de l'interprétation qui sera donnée à la notion de traitement et, par là, du nombre de déclarations à effectuer. De même, les moyens en personnel sont faibles et les membres se consacrant à temps plein à la Commission peu nombreux (199).

4.3. Les compétences

89. — La Commission qui ne disposait que des compétences qui lui étaient attribuées par les réglementations sectorielles (200) voit son pouvoir sensiblement élargi par la récente loi. Dans l'accomplissement de sa mission de protection de la vie privée, cette dernière lui a confié de multiples fonctions.

En premier lieu, elle reçoit des maîtres de fichier les déclarations des traitements automatisés de données à caractère personnel et tient le registre public constitué sur base de celles-ci (201). Le registre forme le répertoire des traitements automatisés (202). Il est supposé permettre à tout individu de connaître les informations qui sont détenues à son sujet et d'identifier les détenteurs de celles-ci. Il devrait donc être suffisamment clair et intelligible, de manière à être à la portée de chaque citoyen.

Deuxièmement, la Commission a une *mission générale de proposition et de conseil* à l'égard des pouvoirs publics. Elle sera amenée à rendre des avis (203) ou des recommandations, soit d'initiative, soit sur demande du gouvernement (204), du parlement, des exécutifs et conseils communautaires et régionaux ou d'un comité de surveillance. Ceux-ci portent sur toute question intéressant la protection de la vie privée à l'égard des traitements de données à caractère personnel (205). Les avis et les recommandations de la Commission doivent être motivés (206). Cette compétence se comprend d'autant mieux que la Commission développera assurément une expertise profitable dans le domaine de la protection des données.

Troisièmement, la Commission a une compétence générale *de contrôle* de l'application de la loi. A cet effet, des compétences particulières lui sont conférées. D'une part, pour autant que la loi n'en décide pas d'une autre manière, elle *examine les plaintes* qui lui sont adressées dans le cadre de ses missions. Cet examen est mené sans préjudice de toute voie de recours devant les tribunaux (207). Si la Commission estime la plainte recevable, elle accomplit toute mission de médiation qu'elle juge utile (208).

D'autre part, elle *dénonce* au procureur du Roi *les infractions* dont elle aurait connaissance (209). Il nous paraît logique que la Commission dénonce, sans distinction aucune, toutes les infractions qui pourraient venir à sa connaissance. Toute autre interprétation conduirait à lui reconnaître le pouvoir de décider s'il est opportun de transmettre l'affaire au procureur du Roi. Cela étant, le fait que la Commission dénonce toute infraction risque de diminuer sa crédibilité en tant qu'organe de médiation.

90. — Trois remarques relatives aux compétences de la Commission doivent encore être formulées. Il y a d'abord lieu de souligner que d'importants pouvoirs d'investigation sont reconnus à la Commission pour l'exécution de ses missions. Elle peut faire opérer des contrôles et vérifications sur le terrain et est habilitée à requérir le concours d'experts (210). Par ailleurs, lorsque la Commission intervient, que ce soit pour prendre une décision, émettre un avis ou édicter des recommandations, elle doit motiver son intervention (211). Enfin, les activités menées par la Commission feront l'objet d'un rapport annuel communiqué aux Chambres (212).

4.4. — Le lien avec les comités de surveillance

91. — Diverses réglementations ont prévu la création de comités de surveillance, sortes de commissions sectorielles, dont le rôle consiste, notamment, à surveiller l'application des principes de protection des données définis dans des domaines particuliers (213).

La loi accorde une attention particulière au partage des compétences entre les comités de surveillance et la Commission. Dans l'hypothèse où un comité est mis sur pied, les pouvoirs de la Commission générale sont réduits d'autant (214). Celle-ci conserve toutefois un droit d'évocation sur les décisions prises par le comité (215). Dans la perspective du respect ou de l'uniformité de l'application des principes généraux, elle peut substituer ses actes à ceux posés par les comités (216). Il n'est pas question d'y voir l'instauration d'une procédure d'appel. La Commission vérifie simplement si les principes généraux de la protection de la vie privée ont été observés et s'ils sont mis en œuvre de manière analogue au sein de chaque institution.

Le lien entre les comités de surveillance et la Commission s'établit, en outre, par le biais de leurs membres respectifs. Il faut, en effet, rappeler que les membres de droit de la Commission sont choisis parmi les comités de surveillance (217) et qu'un membre de la Commission peut assister, avec voix consultative, aux séances des comités (218).

(198) Article 17, § 9.

(199) Le Président exerce ses fonctions à temps plein (art. 26).

(200) Les compétences de la Commission étaient limitées à des domaines particuliers du secteur public (loi du 8 août 1983 organisant un registre national des personnes physiques (*M.B.*, 21 avril 1984) modifiée par la loi du 19 juillet 1991 (*M.B.*, 3 sept. 1991) et arrêté royal n° 141 du 30 décembre 1982 créant une banque de données relative aux membres du personnel du secteur public), aux secteurs de la sécurité sociale (loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale), de la circulation routière (loi du 18 juillet 1990 modifiant la loi relative à la police de la circulation routière et celle relative aux conditions techniques auxquelles doivent répondre tout véhicule de transport par terre, ses éléments, ainsi que les accessoires de sécurité (*M.B.*, 8 novembre 1990) et du crédit à la consommation (loi du 12 juin 1991 relative au crédit à la consommation modifiée par la loi du 12 juillet 1992).

(201) Article 18.

(202) Rappelons que lorsque la Commission estime qu'un fichier manuel est susceptible de porter atteinte à la vie privée, elle peut exiger du maître du fichier qu'il le déclare (art. 19).

(203) Si l'avis est entaché d'irrégularité, un recours en annulation contre la décision peut être exercé. Il s'agit, en principe, d'une formalité substantielle. (*Doc. parl.*, Sén., sess. extr. 1991-1992, p. 52).

(204) Rappelons que la loi prévoit l'avis obligatoire de la Commission dans divers articles.

(205) Article 29, § 1er.

(206) Articles 30, § 3 et 31, § 4. Lorsque la recommandation s'adresse à un maître de fichier, ce dernier a le droit de faire connaître son point de vue (art. 30, § 2).

(207) Article 31, § 1er.

(208) Si la médiation aboutit, la Commission dresse un procès-verbal dans lequel la solution retenue est détaillée. En l'absence de conciliation, elle émet un avis sur le caractère fondé de la plainte (art. 31, § 3).

(209) Article 32, § 2. Tout comme pour la compétence en matière d'examen des plaintes, ce pouvoir revient à la Commission à moins que la loi n'en dispose autrement. La réalité visée par l'exception légale concerne le pouvoir d'instruction des plaintes confié aux comités de surveillance institués par les réglementations particulières. Il s'agit d'éviter que ce pouvoir ne soit « annihilé par des dénonciations prématurées au parquet par la Commission ». Voy. l'exposé des motifs (*op. cit.*, p. 28) et l'avis du Conseil d'Etat (*op. cit.*, p. 63).

(210) Article 32, § 1er.

(211) Articles 30, § 3 et 31, § 4. Lorsque la recommandation s'adresse à un maître de fichier, ce dernier a le droit de faire connaître son point de vue (art. 30, § 2°).

(212) Article 32, § 2.

(213) Le comité de surveillance institué par la loi relative à la Banque-carrefour de la sécurité sociale se charge plus précisément de vérifier que les communications de données se fassent conformément aux dispositions légales et que les mesures de sécurité prévues soient bien observées.

(214) Lorsque la Commission reçoit une doléance ou une requête en matière de sécurité sociale, elle saisit le comité, voy. sur ce sujet le premier rapport d'activité du comité de surveillance (*Rapport d'activité 1992, op. cit.*, p. 41).

(215) Article 44 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale. Pour que le droit d'évocation puisse s'exercer, le comité de surveillance doit porter à la connaissance de la Commission toute demande d'avis, toute requête ou plainte qui lui est adressée. Article 72, § 5, al. 5, de la loi du 12 juin 1991 relative au crédit à la consommation. Pour plus de détails sur la nature de ce droit d'évocation et sur la manière dont il doit être exercé, voy. Commentaire de l'article 44, *Doc. parl.*, Ch. repr., sess. ord., 1988-1989, 899/1 et le premier rapport du comité de surveillance de la Banque-carrefour de la sécurité sociale (*op. cit.*, pp. 40 et s.).

(216) La Commission doit intervenir dans un délai de 30 jours (art. 44, al. 5, de la loi du 15 janv. 1990).

(217) Le président et un membre du comité de surveillance de la Banque-carrefour sont membres de droit de la Commission de la vie privée (art. 44, al. 1er, de la loi du 15 janvier 1990). Il en sera de même en ce qui concerne le comité de surveillance institué par la loi relative au crédit à la Consommation (art. 72, § 5, al. 1er, de la loi du 12 juin 1991).

(218) Article 45 de la loi du 15 janvier 1990.

4.5. — Remarques finales

92. — Les pouvoirs de la Commission ne sont pas extrêmement étendus. Bien que la loi lui accorde des pouvoirs d'investigation, elle ne lui reconnaît pas de réel pouvoir de décision. Son avis est fréquemment requis, mais il n'est pas prévu qu'il doit être conforme. De plus, aucun pouvoir réglementaire ne lui est reconnu (219). La Commission constitue, cependant, un lieu privilégié de discussion et de négociation avec les secteurs concernés. Jouissant de la compétence d'émettre d'initiative des avis et recommandations, elle devra en user sachant que ceux-ci auront d'autant plus de chance d'être pris en compte par leurs destinataires qu'ils auront, au préalable, fait l'objet d'une véritable négociation avec ceux-ci.

5. — LES SANCTIONS PENALES ET L'ENTREE EN VIGUEUR

5.1. — Les sanctions pénales

93. — Le chapitre VIII de la loi prévoit un grand nombre de sanctions pénales en cas de violation des dispositions mises en place. Un commentaire exhaustif de celles-ci sortirait du cadre de cette étude. Nous nous limiterons donc à décrire les grandes lignes de ce régime répressif.

94. — Les peines prévues sont très diverses. Les peines principales consistent en des amendes dont le montant peut varier de 100 F à 100.000 F (220) selon le délit. En cas de récidive, l'article 41, § 3, prévoit la possibilité pour le juge de prononcer au choix une amende et/ou une peine d'emprisonnement de trois mois à deux ans.

95. — Les peines accessoires apparaissent comme particulièrement adaptées à la réalité qui nous occupe. Elles présentent un caractère dissuasif certain au cas où le maître du fichier est une personne morale (221). Ainsi, le juge pourra prononcer la confiscation des supports matériels des données qui forment l'objet de l'infraction (disquettes, bandes magnétiques, etc.) à l'exclusion des ordinateurs eux-mêmes ou de « tout autre matériel » (222). Le but est ici d'éviter de bloquer l'activité de l'entreprise ou de l'administration (223). Les objets confisqués doivent être détruits lorsque la décision est coulée en force de chose jugée (224). Le juge peut aussi ordonner l'effacement des données (225). Il a encore la possibilité d'ordonner « l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'il détermine, aux frais du condamné » (226). Notons que le maître du fichier ou son représentant en Belgique est civilement responsable du paiement des amendes auxquelles son préposé ou mandataire a été condamné (227).

Le juge pourra enfin interdire à la personne condamnée de gérer, personnellement ou par personne interposée tout traitement de données à caractère personnel. La durée de cette interdiction ne peut toutefois excéder deux années (228).

Ces peines peuvent s'avérer extrêmement lourdes. L'exposé des motifs les justifiait par l'objet particulier de la législation : la défense d'un droit fondamental de l'individu (229). Le taux maximum de l'amende devrait permettre de combattre efficacement les infractions commises par les grandes entreprises.

96. — Le texte des articles 38 et 39 désigne le plus souvent l'agent pénalement responsable devant la loi par l'expression « le maître du fichier, son représentant en Belgique, son préposé ou mandataire ». L'imputabilité légale de l'infraction au maître du fichier ou à son représentant en Belgique s'explique par le fait que la loi met expressément à leur charge la plupart des obligations découlant du système de protection. Les sanctions pénales qui punissent la violation de ces obligations ont donc vocation à frapper ces mêmes personnes. Dans ce contexte, l'imputabilité du préposé paraît plus étrange; c'est le seul cas où la loi y fait expressément référence. La lecture des travaux parlementaires révèle que l'ajout des termes « préposé ou mandataire » ne vise qu'à rencontrer l'hypothèse où le maître du fichier est une personne morale. Le droit commun trouve alors à s'appliquer (230). Le juge devra rechercher la personne physique qui, au sein de la personne morale, était chargée de mettre en œuvre l'obligation légale (231). Cette personne physique pourrait être un mandataire de la personne morale ou un de ses préposés. Serait-il possible de la sanctionner lorsqu'elle commet une faute personnelle en dehors de son activité professionnelle normale ? Il nous semble que s'impose une réponse affirmative, l'incrimination légale visant explicitement le préposé ou le mandataire (232) (233).

Si le maître du fichier est une personne physique, c'est à lui que l'infraction sera imputée. Si un préposé a commis matériellement l'infraction (234) dans le cadre normal de ses tâches d'exécution, le maître du fichier ne répondra pas du fait d'autrui et pourra même, le cas échéant, échapper à la répression. En effet, s'il est vrai que toute infraction suppose une faute, le maître pourra se justifier en prouvant qu'il n'en a pas commise; tel serait le cas selon nous « s'il a pris toutes les précautions qu'un homme normalement prudent et diligent aurait prises dans les mêmes circonstances » ou « s'il a délégué, sans fraude ni faute, à une autre personne la responsabilité que la loi lui confère » (235). Le préposé pourrait-il être poursuivi dans ce cas ? Vraisemblablement puisqu'il est mentionné dans la liste des agents à qui l'on peut imputer l'infraction (236). A l'opposé, si le maître du fichier ne peut exciper d'aucune cause de justification, il répondra de sa propre faute. Il aura alors permis à son préposé de violer des obligations qui étaient mises légalement à sa charge et aura commis un manquement à son devoir de surveillance, de direction et de contrôle c'est-à-dire une faute qui est légalement incriminée (237).

97. — Dans trois cas (238), l'imputabilité légale des faits incriminés est implicite. Le législateur utilise l'expression « quiconque ». Il s'agit des violations de l'article 4, §§ 1er et 2 (régime de la collecte), des articles 21 et 22 (régime des flux transfrontières et des intercon-

(219) Le professeur Rigaux émet l'hypothèse que l'absence de pouvoir réglementaire attribué à la Commission provient de ce qu'« un tel pouvoir peut difficilement être attribué à une commission indépendante dans un système de démocratie parlementaire où seul le gouvernement est responsable devant les Chambres législatives de l'action réglementaire » (F. Rigaux, « La protection de la vie privée à l'égard des données à caractère personnel », *op. cit.*, p. 70).

(220) A majorer par le montant des décimes additionnelles s'élevant à 990 FB depuis la loi du 26 juin 1992 portant diverses dispositions sociales (art. 4), (*M.B.*, 30 juin 1992, p. 14843).

(221) Comparer en droit de l'environnement, F. Van Remoortere, « La question de la responsabilité pénale des personnes morales en droit de l'environnement », *Rev. dr. pén.*, 1991, pp. 311 à 371.

(222) Article 41, § 1er.

(223) Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Ch. rep., sess. extr. 1991-1992, n° 413/12, p. 70.

(224) Article 41, § 1er, al. 4.

(225) Article 41, § 1er, al. 1er; remarquons que « la confiscation ou l'effacement peuvent être ordonnés même si les supports matériels des données à caractère personnel n'appartiennent pas au condamné » (art. 41 § 1er, al. 2).

(226) Article 40.

(227) Article 42; pour une évaluation de cette technique voy. F. Van Remoortere, *op. cit.*, pp. 328 et s. et références citées.

(228) Article 41, § 2.

(229) *Doc. parl.*, Ch. repr., sess. ord. 1990-1991, n° 1610/1, p. 30.

(230) On peut se demander si une telle précision était nécessaire.

(231) Voy. à ce propos J. Detienne, *Droit pénal des affaires*, Bruxelles, De Boeck, 1989, pp. 377 et s. et spéc. n° 886 et références citées.

(232) J. D'Haenens, « La responsabilité pénale des personnes morales », *Annales de droit de Louvain*, 1983, p. 62, n° 4.

(233) Cette volonté semble avoir été affirmée explicitement lors des travaux qui eurent lieu au sein de la Commission de la justice du Sénat en présence du ministre. Un membre y déclare, en effet, que l'« on ne pourra, en tout cas, poursuivre le préposé sur base de l'article 38 si le maître du fichier est une personne physique, *à moins qu'il n'ait été coauteur ou complice*. C'est le droit commun qui est applicable » (Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Sén., sess. extr. 1991-1992, n° 445/2, p. 55). Le législateur semble oublier l'hypothèse où le préposé commet seul l'infraction. Ainsi en serait-il, s'il fait une copie des données pour les vendre à l'insu du maître du fichier.

(234) Sans que l'élément moral de celle-ci lui soit imputable.

(235) J. Messinne, « Questions juridiques à propos du droit de l'environnement en Belgique », *R.D.C.*, 1992, p. 666; Voy. aussi dans le même sens, R. Legros, « Le droit pénal dans l'entreprise », *J.T.*, 1977, pp. 175 et 176; pour une vision plus critique de la responsabilité du « décideur », voy. C. Hennau et J. Verhaegen, *Droit pénal général*, Travaux de la Faculté de droit, U.C.L., 1991, p. 227 et spéc. n°s 293 à 296.

(236) Pour autant qu'il ait bien commis une faute.

(237) R. Legros, *op. cit.*, p. 175.

(238) Articles 39, 1° et 2°; 39, 11° et 12°; 39, 3°.

nexions de traitements) ainsi que de l'article 32 (entraves aux vérifications de la Commission ou de ses membres et experts). Dans ces cas, le juge pourra condamner tant le maître du fichier que son représentant, préposé, mandataire ou même un tiers.

98. — Remarquons enfin que le texte ne précise rien en ce qui concerne l'élément moral requis (239). Selon le droit commun, ce silence s'interprète comme l'exigence d'une intention (240) (*dolus generalis*). Un simple défaut de prévoyance ou de précaution ne suffit généralement pas pour que le délit puisse être imputé à l'agent.

5.2. — L'entrée en vigueur

99. — Deux arrêtés royaux adoptés le 28 février 1993 (241) sont venus préciser les différentes étapes de l'entrée en vigueur du texte de loi. Cette entrée en vigueur se caractérise par une volonté de souplesse, traduite à deux niveaux. Une distinction est tout d'abord faite entre les traitements existant au moment de l'entrée en vigueur des différentes dispositions de la loi et les traitements à venir (242). D'autre part, la mise en œuvre du nouveau régime juridique dont la loi est porteuse est progressive, afin de prendre en compte les contingences matérielles et organisationnelles découlant de l'application de certaines dispositions, et de permettre au pouvoir réglementaire de prendre les mesures d'exécution nécessaires. L'échelonnement dans le temps proposé par l'arrêté royal n° 1 présente surtout l'avantage d'assurer l'application immédiate des principes protecteurs de base, sans suspendre celle-ci à la mise en œuvre obligatoirement plus lente de certaines dispositions.

100. — L'entrée en vigueur de la loi se présente en quatre temps. Dès le 1er avril 1993, des dispositions « techniques » comme les définitions et la détermination du champ d'application entrent en application, de même que les deux principes protecteurs fondamentaux : le droit de chaque individu au respect de sa vie privée lors du traitement de ses données à caractère personnel (contenu à l'article 2) et le principe de finalité (article 5). C'est aussi à cette date qu'entrent en vigueur les dispositions relatives à la mise en place de la Commission de la protection de la vie privée. Le 1er septembre 1993 voit essentiellement l'application des dispositions concernant les droits des personnes fichées et les obligations corrélatives des ficheurs. Les régimes particuliers accordés à certaines catégories de données (données sensibles, médicales et judiciaires) sont également d'aplication à ce moment. Troisième étape, le 1er mars 1994 entraîne l'entrée en vigueur de la formalité de déclaration des traitements automatisés auprès de la Commission et la constitution par celle-ci du registre des déclarations reçues. Enfin, au 1er septembre 1994, des dispositions exigeant un plus long délai car nécessitant la prise de mesures techniques ou organisationnelles, seront d'application. Il s'agit de l'obligation pour le maître du fichier de prendre les mesures requises pour garantir la sécurité des données et de veiller à limiter l'accès interne au traitement et la communication des données. Il s'agit aussi de la disposition concernant la communication des données médicales.

6. — CONCLUSION GENERALE

101. — On ne peut que saluer l'initiative du gouvernement et le vote de la loi du 8 décembre 1992. Vingt ans après les premières discussions parlementaires, le citoyen semble jouir enfin d'une protection; un équilibre se dessine entre l'intérêt des maîtres de fichier à utiliser les nouvelles technologies de l'information et le respect de la vie privée des individus. Trois questions s'imposent cependant.

A-t-on légiféré pour le présent ? Le premier objectif de la loi est de garantir la protection de la vie privée des personnes concernées par les données. Le régime légal mis en place à cet effet manque parfois de souplesse. Le système de protection repose sur trois acteurs : l'individu, le maître du fichier et la Commission. Il semble que le législateur n'a pas toujours apprécié correctement le rôle qu'il entend leur faire jouer.

La capacité de l'individu concerné par les données traitées à mettre en œuvre ses nouveaux droits ne doit pas être surestimée. Mal informé, il se préoccupe peu des multiples possibilités d'utilisation des données qui le concernent. Bien que la loi prévoie différentes mesures afin de remédier à cette situation (une information lors de la collecte, lors du premier enregistrement, etc.), il n'en reste pas moins qu'en l'absence d'un réel débat de société, l'individu risque de ne pas être conscient des menaces résultant du traitement de ses données.

Même si le respect des obligations est garanti par des sanctions pénales, en l'absence de moyens de contrôle suffisamment efficaces, la réalité de la protection risque d'être étroitement liée à la bonne volonté des maîtres du fichier. Les dispositions légales, particulièrement techniques, ne sont pas faciles à lire. En outre, les obligations prévues impliquent de lourdes charges administratives dont l'intérêt et la portée ne ressortent pas toujours avec évidence. Il suffit de rappeler la formalité de déclaration systématique de chaque traitement automatisé.

Les dispositions de la loi contiennent de nombreuses zones d'ombres. La Commission de la vie privée se voit chargée par le législateur d'apporter les éclaircissements nécessaires. Pourra-t-elle faire face à cette périlleuse mission d'interprétation à laquelle s'ajouteront des tâches administratives pesantes. Tâches qui écarteront la Commission de sa mission première : le contrôle du respect de la protection mise en place. On peut douter que la Commission dispose des moyens humains et financiers de la politique qu'on entend lui faire mener.

A-t-on légiféré pour l'avenir immédiat ? La loi est-elle compatible avec ce qui se dessine à l'horizon européen ? Le législateur ne devra-t-il pas, dans un futur proche, la remettre sur le métier et adapter son texte ? Sans être véritablement incompatibles, la loi belge et la proposition de directive présentent de nombreuses divergences notamment dans la définition des axes de protection. On relèvera, par exemple, que la directive allège considérablement l'obligation de déclaration et accorde une grande importance au consentement de l'individu. Ces divergences risquent de s'accentuer encore dans la version définitive de la législation européenne.

A-t-on légiféré pour l'avenir ? Les termes de la loi ne sont-ils pas liés à un contexte technique donné ? Pourront-ils appréhender une réalité technologique en constante évolution ? Le législateur n'est pas tombé dans le travers de ce que l'on a appelé « la première génération » des lois de protection des données. La protection ne se réfère pas à des fichiers centralisés et physiquement localisables. Conscient de la rapidité et de l'imprévisibilité des innovations, le législateur a entendu saisir l'utilisation des données en elle-même. Certaines interrogations subsistent cependant. Un exemple suffira. Les systèmes d'information sont de plus en plus intégrés. Chaque utilisateur isolé peut créer des nouvelles applications à partir du même ensemble de données. Comment, dans ce cas, contrôler efficacement le respect du principe de finalité ?

Il reste à saluer l'œuvre de sensibilisation dont la loi est porteuse. L'information et l'éducation des différents acteurs constituent la clé de l'efficacité du régime de protection mis en place. Le rôle de la Commission de la protection de la vie privée est à ce niveau prépondérant. Les solutions à apporter aux multiples problèmes d'interprétation de la loi doivent se trouver dans une concertation franche et ouverte entre les membres de la Commission, d'une part, et les différents acteurs concernés, d'autre part. La recherche d'un équilibre entre les multiples intérêts antagonistes passera désormais, par ce nouveau lieu de discussion. Dès aujourd'hui, le ficheur doit, cependant, avoir conscience qu'il ne peut se faire complice de la machine au détriment du fiché. A ce dernier il revient d'être vigilant, afin de protéger, avec les moyens dont il dispose dorénavant, cet élément essentiel de sa personnalité : le respect de son image informationnelle.

Marie-Hélène BOULANGER,
Cécile de TERWANGNE
et Thierry LEONARD

(239) Si ce n'est dans le cas de l'article 39, 5°, *in fine* (« (...) *ou donné sciemment des renseignements inexacts ou incomplets* »).

(240) C. Hennau et J. Verhaegen, *op. cit.*, pp. 268 et s. et références citées.

(241) Arrêté royal n° 1 du 28 février 1993 fixant la date d'entrée en vigueur des dispositions de la 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 mars 1993, p. 5816 et arrêté royal n° 2 fixant le délai dans lequel le maître du fichier doit se conformer aux dispositions de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel pour les traitements existant au moment de l'entrée en vigueur de ces dispositions, *M.B.*, 18 mars 1993, p. 5818.

(242) Prévoir un délai d'adaptation pour les traitements existant au moment de l'entrée en vigueur nous ramène à la difficulté désormais classique d'interpréter le concept de traitement et plus particulièrement, dans ce cas, de traitement existant. Pour le détail, voy. les arrêtés royaux n^{os} 1 et 2 du 28 février 1993.