

La nouvelle législation belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*

The new Belgian law relating to the protection
of privacy concerning the processing
of personal data

par Bernard HANOTIAU
Avocat au Barreau de Bruxelles

Résumé. Après un long processus, la Belgique s'est enfin dotée, le 8 décembre 1992, d'une loi sur la protection de la vie privée à l'égard des traitements de données à caractère personnel. Son entrée en vigueur s'échelonne du 1er août 1993 jusqu'au 1er septembre 1994.

Cette loi fait un compromis entre un système répressif et un système préventif et reprend tous les grands principes de la convention 108 du Conseil de l'Europe.

Le premier chapitre regroupe les définitions et les exceptions qui vont préciser le champ d'application de la loi. Ainsi, nous y retrouvons la définition de notions fondamentales telles que les données à caractère personnel, le fichier, le traitement automatisé et la tenue d'un fichier manuel.

Le chapitre 2 est consacré aux principes de base de la loi. L'article 2 pose le principe du droit au respect de la vie privée des personnes physiques. Ainsi, le traitement des données à caractère personnel est autorisé aussi longtemps qu'il respecte les finalités déclarées. Ces finalités sont strictement définies par l'article 5 et notamment, elles doivent être déterminées, légitimes et adéquates. Les données dites sensibles bénéficient d'une protection encore plus importante, puisque le traitement, dans ce cas, nécessite une autorisation préalable par arrêté royal, après avis de la Commission pour la protection de la vie privée. Les données médicales et judiciaires sont spécialement traitées par la loi.

Le chapitre 3 traite des obligations du maître du fichier. Celui-ci doit informer les personnes

qu'elles vont être fichées. Cette information doit être simultanée au traitement, à moins que ce ne fût fait au moment de la collecte. Le traitement doit être préalablement déclaré à la Commission pour la protection de la vie privée. Le maître du fichier doit également assurer la mise à jour de ces données, les corriger et veiller à leur sécurité contre tout acte de piratage ou de destruction.

Par ailleurs, la personne fichée bénéficie des droits définis au chapitre 4. Il s'agit du droit d'accès et de rectification, et éventuellement de la possibilité de consulter le fichier des fichiers. Par contre, la personne fichée ne peut s'opposer à l'utilisation des données la concernant. La Commission pour la vie privée est la garante de ces droits et dispose à ce titre de pouvoirs étendus. Les contraventions à la loi sont susceptibles d'être sanctionnées pénalement et civilement et dans certains cas un recours en référé peut être exercé.

Summary. After a lengthy period, Belgium finally equipped itself on 8th December 1992 with a privacy protection law with regard to the processing of personal data. The law will enter into effect over a period ranging from 1st August 1993 to 1st September 1994.

This law is a compromise between a repressive and a preventive system and takes up all the principles of the Council of Europe's Convention n° 108.

The first chapter groups the definitions and the exceptions which stipulate the law's scope. We find the definition of such fundamental notions as

pe
orglav
inc
Thu
as
The
pa
am
pr
pr
mis
ciahol
he
giv
is
mu
sio
to
ensdel
ces
cor
car
for
has
car
in
be199
vée
ract
long
succGrè
nav
tière
lativ
trait
pers
dire
dep
belg
tenu
vau
part
saire

personal data, files, automatic processing or the organisation of a manual file.

Chapter 2 covers the basic principles of the law. Article 2 sets down the legal principal of an individual's right to have his private life respected. Thus, the processing of personal data is possible as long as it is done within the declared aims. These aims are strictly defined by article 5 and, in particular, they must be determined, legitimate and adequate. Sensitive data have even greater protection because processing requires prior approval by royal decree after consulting the Commission for privacy protection. Medical and judicial data are specifically covered by the law.

Chapter 3 covers the obligations on the file holder. He must inform the person concerned that he is going to be listed. This information must be given at the same time as the processing, unless it is made when the data is collected. Processing must also be previously declared to the Commission for privacy protection. The file holder also has to ensure that the data is up-dated, correct it and ensure that it is not subject to piracy or destruction.

Further, the listed person is entitled to all rights defined in chapter 4. These include right of access, amendments, and even the possibility of consulting the list of files. However, the person cannot forbid the use of his data. The Commission for privacy protection guarantees these rights and has wide-reaching powers. Infractions of the law can give rise to civil and criminal proceedings and in certain cases urgent interim proceedings can be brought.

1. Le Parlement belge a adopté le 8 décembre 1992 une loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. L'aboutissement d'une très longue évolution, différents projets s'étant en effet succédés depuis près de vingt ans.

La Belgique était avec l'Espagne, l'Italie et la Grèce un des derniers pays de l'Europe communautaire à ne pas avoir de législation en la matière. Or, la Convention du Conseil de l'Europe relative à la protection de la vie privée à l'égard du traitement automatisé des données à caractère personnel a été signée le 28 janvier 1981, c'est-à-dire il y a plus de 10 ans et est entrée en vigueur depuis le 1er octobre 1985. L'adoption d'une loi belge était devenue d'autant plus urgente compte tenu, d'une part du degré d'avancement des travaux sur la proposition de directive CEE et, d'autre part, du fait qu'elle constituait un préalable nécessaire à la ratification des accords de Schengen.

L'absence d'une législation sur la protection de la vie privée était par ailleurs d'autant plus paradoxale que la Belgique avait été un des pionniers de la protection de la vie privée : le premier projet belge, oeuvre du Ministre Vanderpoorten, avait inspiré plusieurs législations étrangères dont la législation suédoise.

2. Quel est le système prévu par la loi ?

Il existe dans les législations nationales deux approches principales : l'approche préventive où tous traitements sont interdits sauf autorisation, et l'approche dite répressive où tout est autorisé mais où la loi instaure un système de contrôle aux termes duquel les abus les plus manifestes sont sanctionnés a posteriori. Dans ce dernier système, la règle générale est la liberté de principe de traiter les données à caractère personnel, soit sous forme manuelle, soit sous forme automatisée.

La loi belge se situe entre les deux extrêmes : elle se caractérise en premier lieu par une approche du type répressif en ce sens que le traitement des données est en principe autorisé. Ce système a été préféré parce que le système dit préventif aurait, selon le législateur, mené à un engorgement rapide et inéluctable de l'organe de contrôle. On s'est fondé notamment sur l'expérience suédoise très significative à cet égard : les Suédois ont en effet été contraints d'opérer un renversement de principe vu le submergement des autorités administratives.

La loi belge ne s'est néanmoins pas bornée à un système purement préventif qui n'assurait qu'un niveau de protection insuffisant. Elle a voulu garantir la transparence des données. A cette fin, elle prévoit notamment que le maître du fichier aura l'obligation de déclarer préalablement à la Commission de la vie privée, la création ou la modification de tout traitement. Celle-ci pourra ainsi tenir à la disposition du public le fichier des fichiers.

Dans la même perspective, le maître du fichier devra informer tout intéressé lors de la collecte ou de l'enregistrement de toute donnée le concernant. Il devra de plus faire suivre toute rectification de données vers les personnes auxquelles des données inexacts, incomplètes ou non pertinentes ont été communiquées.

Participent à cette idée de prévention dans un système répressif les nombreuses obligations qui sont faites au maître du fichier par la loi.

Enfin, pour les cas où un risque particulier d'atteinte à la protection de la vie privée existe, le législateur en est revenu à une conception plus

préventive. En effet, les données dites sensibles et judiciaires ne peuvent être traitées sauf autorisation que par arrêté royal après avis de la Commission de la vie privée. Les données médicales font également l'objet d'un sort particulier eu égard à leur grande spécificité.

Cette approche s'inscrit parfaitement dans l'optique du seul instrument international qui est contraignant à l'heure actuelle, la Convention 108 du Conseil de l'Europe.

Chapitre I - Champ d'application

L'on distinguera successivement le champ d'application *ratione personae*, *ratione materiae* et *ratione loci*.

1. *Ratione personae*

L'article 2 de la loi dispose que toute personne physique a droit au respect de sa vie privée lors du traitement des données à caractère personnel qui la concernent.

Le paragraphe 5 de l'article 1 précise quant à lui que sont réputées à caractère personnel les données relatives à une personne physique identifiée - c'est-à-dire nommément désignée - ou identifiable - c'est-à-dire par exemple une personne qui serait désignée par un numéro avec clé de conversion permettant de déterminer l'identité de la personne.

2. *Ratione materiae*

La loi belge ne concerne ni la banque de données, ce qui était l'objet du premier projet Vanderpoorten, ni le fichier, ni les données en soi. Elle concerne le traitement de données. On a donc délibérément opté pour l'élément dynamique.

L'article 3 de la loi dispose qu'elle s'applique à la tenue d'un fichier manuel et à tout traitement automatisé. Aucune distinction n'est faite par ailleurs entre secteur public et secteur privé.

a) La loi définit la notion de traitement automatisé comme étant 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.

b) La loi s'applique en outre à la tenue de fichiers manuels.

Le paragraphe 4 de l'article 1 précise qu'il faut entendre 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.

Certes, les fichiers manuels sont en voie de disparition. Le législateur a voulu néanmoins éviter le risque que l'on imprime sur fichiers les traitements automatisés pour obtenir un fichier manuel et échapper ainsi au prescrit de la loi. C'est pour cette raison que les fichiers manuels ont été maintenus dans le champ d'application de la réglementation même s'il est exact que la Convention de Strasbourg ne s'applique pas à ces fichiers.

L'on précisera enfin que la notion de fichier est définie par le paragraphe 2 de l'article 1 comme étant à un ensemble de données à caractère personnel, constitué et conservé suivant une structure logique devant permettre une consultation systématique.

c) Jusqu'où s'étend le champ d'application de la loi ?

L'on a évoqué au cours des travaux parlementaires la possibilité d'établir des traitements automatisés à partir de bandes vidéo où l'on aurait par exemple, lors d'un congrès, filmé l'entrée des membres d'un parti politique. La question a également été posée de savoir si l'enregistrement photographique d'un excès de vitesse par un radar automatique entre dans le champ d'application de la loi. Le Ministre a répondu que les photos ou images photographiques entraînent dans le champ d'application de la loi : il s'agit en effet de données se rapportant à des personnes physiques identifiées ou identifiables. Il en est de même, a-t-il été précisé, pour des empreintes digitales ou des données génétiques.

3. *Ratione loci*

Au niveau territorial, la loi s'applique à la tenue d'un fichier manuel en Belgique et 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.

En fait, la loi est applicable dès qu'on peut accéder au traitement en Belgique si aucune autre intervention humaine n'est nécessaire. Ainsi, si un traitement est accompli sur 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. Que l'ordinateur ait à cette fin recours à des télécommunications, à une ligne téléphonique ordinaire, à une

ligne privée intégrée au réseau qui accomplit le traitement, est sans influence. De même, le fait que l'ordinateur utilise un "personal computer", un minitel ou un simple téléphone. Le champ d'application est donc partiellement extensif.

Par contre, le traitement doit être considéré comme n'étant plus directement accessible en Belgique par des moyens qui lui sont propres lorsque l'opérateur établi en Belgique doit téléphoner à un collègue en Allemagne qui, lui, dispose d'un terminal permettant d'accéder au système.

4. Les exceptions

La loi prévoit des exceptions à son champ d'application. Elles sont contenues dans l'article 3, paragraphes 2 et 3.

a) Aux termes de la première exception, la loi ne s'applique pas au traitement de données à caractère personnel gérées par des personnes physiques qui, de par leur nature, sont destinées à un usage privé, familial ou domestique et conservent cette destination. Sont visés principalement les fichiers constitués par des personnes privées sur leur "personal computer". Mais jusqu'où s'étend cette exception ? Ainsi, au cours des travaux préparatoires, un membre de la Commission parlementaire avait posé la question de savoir ce qu'il fallait entendre par les termes usage privé et il donnait à cet égard plusieurs exemples : un commerçant ayant un fichier de clients, fidèles, tombe-t-il sous l'application de la loi ? De même, le fichier des élèves d'une école ? Ou encore une association sportive sans but lucratif qui a mis la liste de ses membres dans son "personal computer" ? Selon le ministre, l'usage d'un fichier automatisé des clients ou des élèves d'une école relève de l'usage professionnel, tandis que pour l'association sportive, il s'agira d'un usage privé. Ont également été cités comme relevant d'un usage professionnel, les fichiers des parlementaires et les registres existants dans les paroisses.

b) La loi ne s'applique pas aux traitements portant 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 par exemple des registres de commerce, de l'état civil, de la conservation des hypothèques, du cadastre.

c) La loi ne s'applique pas aux traitements portant exclusivement sur des données à caractère personnel dont la personne à laquelle elles se rapportent assure ou fait assurer la publicité pour autant que le traitement respecte la finalité de la publicité. Tel est le cas des annuaires télé-

phoniques des lors qu'ils sont utilisés dans le respect de la finalité qui leur est propre.

d) La loi ne s'applique pas aux traitements de données à caractère personnel effectués conformément à la loi du 4 juillet 1962 relative à la statistique publique, à l'exception de ceux qui sont visés à l'article 2, C, al. 2 et aux articles qui s'y réfèrent, ainsi qu'à l'article 5.

e) La loi prévoit enfin que certains articles, les articles 4, 6 à 10, 12, 14, 15, 17, 18, 20 et 31, paragraphes 1 à 3, ne sont pas applicables aux traitements de données à caractère personnel, nécessaires pour l'exercice de leurs missions, gérés par l'administration de la sûreté de l'Etat, du Ministère de la justice et le service général du renseignement et de la sécurité du Ministère de la défense nationale. Bien entendu, ce sont ici les impératifs supérieurs de sécurité qui justifient cette exception.

Il est certain, d'autre part, que la sûreté de l'Etat et le service général du renseignement et de sécurité de l'armée demeurent soumis aux obligations générales, à savoir l'article 2 (respect de la vie privée) et l'article 5 (respect des finalités). Ces services ne peuvent donc collecter et traiter des informations que si cette démarche répond aux finalités définies jusqu'ici par les ministres compétents sous le contrôle du Parlement. D'autre part, bien que l'administration de la sûreté ne soit pas tenue de faire une déclaration préalable au sens de l'article 17, le citoyen dispose à l'égard des fichiers de cette administration d'un droit d'accès et de rectification indirecte qui s'exerce par le biais de la Commission de la protection de la vie privée.

Chapitre II - Les principes de base de la loi

Les principes de base de la loi sont contenus dans les articles 2 et 5.

L'article 2 dispose que toute personne physique a droit au respect de sa vie privée lors du traitement des données caractère personnel qui la concernent. Le législateur n'a pas tenté de définir la notion de vie privée. Elle constitue une valeur qui a une signification fondamentale, importante et permanente dans nos systèmes juridiques. Il s'agit, par ailleurs d'un concept essentiellement relatif qui dépend des traditions culturelles et d'un environnement social et même économique.

D'autre part, l'article 5 précise que 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.

Le traitement des données à caractère personnel est donc autorisé aussi longtemps qu'il respecte les finalités qui ont été déclarées pour le traitement.

Ces deux articles appellent un certain nombre de commentaires.

1. L'étendue de la protection prévue par l'article 2

La loi étend sa protection aux personnes physiques identifiées ou identifiables. En revanche, si les personnes morales doivent respecter la loi, elles ne peuvent bénéficier de sa protection. Elles ne sont pas protégées en tant que telles. L'article 3 de la Convention du Conseil de l'Europe permet à tout Etat d'étendre son application à des informations afférentes à des groupements, associations, fondations, etc. Cette possibilité n'a pas été reprise dans la loi belge. Mais la loi s'applique-t-elle lorsque, constituant une banque de données de sociétés, on y mentionne le nom d'individus ? Le ministre de la justice a été extrêmement clair à cet égard : "Si les données relatives à la personne morale contiennent des informations relatives à des personnes physiques (par exemple, les noms des administrateurs d'une société ou des membres d'une association sans but lucratif), ces dernières bénéficient de la totalité de la protection donnée par la loi en projet".

Nous verrons toutefois ultérieurement que la réponse doit être nuancée dans la mesure où la loi prévoit des exceptions à l'obligation d'information lorsqu'il existe une relation contractuelle entre le maître du fichier et la personne fichée.

2. Le champ d'application de l'article 5 : le respect de la finalité du traitement

L'article 5 dispose que les finalités des traitements doivent être déterminées et légitimes et que les données doivent être adéquates, pertinentes et non excessives par rapport à ces finalités.

Le législateur ne dit donc pas que les données doivent être exactes. Or, l'article 12 qui prévoit le droit de rectification, précise que toute personne a le droit à la rectification d'une donnée inexacte qui la concerne. Comment expliquer cette différence ? En fait, au cours des travaux préparatoires, un amendement avait été proposé, tendant à préciser que les données recueillies devaient être exactes et, si nécessaire, mises à jour. Cette garantie figure effectivement à l'article 5 de la

Convention de Strasbourg. Cet amendement n'a finalement pas été maintenu, dans le souci de respecter la philosophie de base. La loi a en effet adopté un système de type répressif : il n'y a donc pas d'obligation légale à ce que les données collectées soient exactes mais, si une donnée collectée présente ce caractère, la personne concernée bénéficiera d'un droit de rectification. Etant donné que la loi est assortie de sanctions pénales, il est certain que si l'on avait inséré les mots "exactes et si nécessaires mises à jour", cette exigence supplémentaire aurait pu donner lieu à des abus, la moindre inexactitude ou l'absence d'une mise à jour mineure pouvant être en effet punie pénalement. Qui va dans le système établi par la loi belge, apprécier si les données sont adéquates, pertinentes et non excessives ? C'est le maître du fichier qui doit en juger en premier lieu ; ensuite la Commission de la vie privée ; enfin, éventuellement, le Parquet, le juge.

Tels sont donc les principes qui sont à la base de la loi : les données peuvent être utilisées, mais uniquement pour des finalités déterminées et légitimes, et elles doivent être adéquates, pertinentes et non excessives par rapport à ces finalités.

Ainsi, l'avocat peut légitimement avoir une banque de données de ses clients. Mais s'il est également parlementaire, il ne peut pas utiliser cette banque de données pour son mailing électoral, à peine de détourner de sa finalité la banque de données.

3. Les données sensibles

A l'instar des données à caractère médical et des données judiciaires, les données sensibles font l'objet d'un traitement particulier à l'article 6 de la loi.

D'une part, le traitement de données à caractère personnel relatives aux origines raciales ou ethniques, à la vie sexuelle, aux opinions ou activités politiques, philosophiques ou religieuses, aux appartenances syndicales ou mutualiste n'est autorisé qu'aux fins déterminées par ou en vertu de la loi. Dans ce dernier cas, la commission pour la protection de la vie privée doit rendre un avis préalable.

Le Roi peut par ailleurs, par arrêté délibéré en Conseil des Ministres, après avis de la Commission de la vie privée prévoir des conditions particulières relatives aux traitements des données sensibles. L'on aperçoit d'emblée les problèmes que la loi pourrait poser aux banques, par exemple, qui traitent des virements d'affiliation à des partis politiques ou des syndicats. La loi n'a en

effet prévu aucune dérogation.

Dans ce cas particulier, comme dans beaucoup d'autres, divers intervenants à la Commission de la Justice ont considéré que le projet donnait un pouvoir de dérogation trop important au Roi. La réponse du gouvernement a été que l'on se trouve, en matière de vie privée, en présence d'un concept difficile à définir et évolutif. Le législateur doit donc adopter un cadre traçant les grands principes dans lesquels d'autres acteurs devront nécessairement se mouvoir. Il n'est pas concevable d'imaginer qu'il faille revenir constamment devant le Parlement pour rencontrer toutes les spécificités qui apparaîtront à l'avenir. C'est pour cette raison qu'une compétence a été offerte à l'exécutif qui ne peut agir qu'en étroite collaboration avec la Commission de la vie privée puisque la plupart des arrêtés royaux devront être précédés d'avis de cette Commission, obligatoirement publiés au Moniteur belge.

Il importe enfin de souligner que l'article 6 précise spécifiquement qu'il n'interdit pas à une association de fait ou à une association dotée de la personnalité juridique, de tenir un fichier de ses propres membres. Il reste que cette autorisation ne dispense pas du respect des dispositions de la loi, notamment l'article 5 prévoyant le respect de finalité légitime et l'article 9 concernant le droit d'information.

4. Les données médicales

Il faut entendre par données médicales toutes 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 (article 7).

L'article 7 de la loi traite de deux types de cas.

a) D'une part, les données médicales à caractère personnel ne peuvent être traitées que sous la surveillance et la responsabilité d'un praticien de l'art de guérir. Toutefois, ces données peuvent être traitées, hors la surveillance et la responsabilité d'un praticien de l'art de guérir, avec le consentement spécial donné par écrit par l'intéressé.

Plusieurs remarques doivent être formulées à cet égard.

- D'une part l'article 7 ne concerne pas uniquement les médecins, comme dans le projet initial, mais aussi les autres praticiens de l'art de guérir, à savoir les dentistes et les pharmaciens. Ceux-ci traitent également des données médicales.

- La dérogation au principe selon lequel les données médicales ne peuvent être traitées que sous la surveillance et la responsabilité d'un praticien de l'art de guérir, lorsque l'intéressé a donné son consentement, se justifie par exemple dans les cas suivants qui ont été énoncés lors des travaux préparatoires :

a) Le cas des règlements de l'ATA qui prévoient que certaines données médicales relatives aux personnes transportées doivent être communiquées au personnel de bord et au personnel chargé de la sécurité des aéroports ; le cas des responsables d'un mouvement de jeunesse qui organisent chaque année un camp et qui doivent pouvoir disposer de certaines données médicales relatives aux jeunes qui leur sont confiés.

b) Sauf dérogation prévue par, ou en vertu de la loi, et dans ce dernier cas après avis de la Commission de la vie privée, il est interdit de communiquer des données médicales à des tiers. Elles peuvent toutefois être communiquées à un praticien de l'art de guérir et à son équipe médicale moyennant consentement spécial donné par écrit par l'intéressé ou en cas d'urgence aux fins de son traitement médical (pour chaque acte médical séparément).

Les dérogations prévues par la loi visent certaines obligations stipulées par la législation en matière de sécurité sociale.

La condition du consentement spécial donné par écrit n'est évidemment pas requise dans les cas d'urgence, aux fins de traitement médical.

5. Les données judiciaires

Le traitement des données judiciaires énoncées à l'article 8 de la loi n'est autorisé qu'aux fins déterminées par ou en vertu de la loi et, dans ce dernier cas, après avis de la Commission de la vie privée.

Un pouvoir réglementaire a également été accordé au Roi, lui permettant de prévoir des conditions particulières relatives au traitement des données judiciaires (article 8 § 2).

L'article 8 § 4 prévoit par ailleurs que les données relatives aux litiges soumis aux Cours et aux Tribunaux peuvent faire l'objet de traitements par des personnes physiques ou morales de droit public ou de droit privé aux seules fins de gestion de leur propre contentieux.

L'on relèvera notamment l'incidence de l'article 8 sur la pratique des grandes surfaces qui fichent les auteurs de vols dans l'intention de transmettre les noms au Parquet en cas de récidive. En principe, le traitement de ces données n'est pas autorisé, sauf si le Roi y déroge par arrêté délibéré au

Conseil des Ministres après avis de la Commission de la protection de la vie privée.

Chapitre III - Les obligations du maître du fichier

1. Le maître du fichier

La définition en est donnée au paragraphe 6 de l'article 1. Par "maître du fichier", on entend la personne physique ou morale ou l'association de fait compétente pour décider de la finalité du traitement des catégories de données devant y figurer. Lorsque la finalité du traitement ou des catégories de données devant y figurer sont déterminées par la loi, le maître du fichier est la personne physique ou morale déterminée par la loi pour tenir le fichier.

Le maître du fichier, personne physique qui n'a pas de domicile en Belgique, doit, pour permettre l'exercice des droits visés aux articles 10 et 12, élire domicile en Belgique.

Le maître du fichier, personne morale ou association de fait dont le siège est situé à l'étranger, doit désigner un représentant en Belgique auprès duquel pourront être exercés les droits visés aux articles 10 et 12.

Ces exigences se justifient par le fait que le maître du fichier est un personnage central, en première ligne pour l'application des sanctions pénales prévues en cas de violation de la loi.

La détermination du maître du fichier ne devrait pas poser de problème dans la pratique. Il importera de déterminer dans chaque cas d'espèce qui dispose réellement du pouvoir de choix et qui n'est qu'un exécutant. Il reste que son identification sera facilitée, sous le contrôle de la Commission pour la protection de la vie privée, par le fait que la déclaration préalable prévue à l'article 17 doit indiquer clairement qui est le maître du fichier.

En pratique, il s'agira souvent d'une personne morale qui, par un de ses organes, décidera de la finalité et, par un autre organe, décidera du contenu.

2. L'obligation d'information ou de transparence

L'obligation d'information du maître du fichier est contenue dans trois articles : 4, 9 et 17.

Elle va normalement s'exécuter au niveau de la collecte des données. L'article 4 dispose en effet que "lorsque les données à caractère personnel sont recueillies sur le territoire belge, en vue d'un traitement effectué ou non en Belgique, auprès de la personne qu'elles concernent, celle-ci doit être

informée" de différents éléments concernant le fichier et, notamment, de l'identité du maître du fichier, le cas échéant de la base légale ou réglementaire de la collecte des données, de la finalité poursuivie et du droit d'accès et de rectification.

Si l'obligation d'information a été exécutée au moment de la collecte des données, il n'y a plus lieu de recommencer à un stade ultérieur. Si toutefois, l'information n'a pu être fournie antérieurement, c'est au moment où la personne est enregistrée pour la première fois dans un traitement déterminé, qu'elle doit en être informée, sauf dans les cas particuliers prévus à l'article 9, la principale exception concernant l'existence d'une relation contractuelle entre la personne concernée et le maître du fichier.

a) Communication de l'information lors de la collecte des données

Les indications prévues aux points 1 à 5 de l'article 4 de la loi doivent figurer sur tous les documents qui seront envoyés à la personne concernée. L'information doit être fournie à l'occasion de chaque traitement.

Faut-il mentionner que la réponse a un caractère obligatoire ou facultatif ? Ce que l'on appelle le principe de loyauté inscrit à l'article 5 de la Convention de Strasbourg, n'a pas été repris dans la loi. Il a été estimé que cela n'était pas nécessaire vu que l'article 4 prévoyait déjà que la personne concernée est informée, le cas échéant, de la base légale ou réglementaire. En effet, ceci devrait lui permettre de savoir si elle a oui ou non l'obligation de répondre au questionnaire qui lui est adressé.

Par ailleurs, l'obligation d'information n'est pas applicable aux traitements de données à caractère personnel visés à l'article 11, 2° à 4° qui concernent des traitements de données à caractère personnel, gérés par des autorités publiques en vue de l'exercice de leurs missions de police judiciaire ou administrative. Ces exclusions se justifient par un intérêt supérieur, à savoir d'ordre public, d'ordre judiciaire ou de maintien de l'ordre. Il est évident que l'on ne peut informer une personne du fait que la police judiciaire réalise à son sujet une enquête parce qu'elle est soupçonnée d'avoir commis une infraction.

L'article 11, 1° n'est pas visé. Il concerne l'hypothèse d'un recensement. Cela signifie qu'en cas de recensement, tout citoyen pourra avoir accès aux données le concernant et demander, le cas échéant, leur rectification. Toutefois, lorsque les données deviendront ultérieurement anonymes, il n'aura plus accès à ces traitements, étant donné

qui
ten
pe
Bel
ce,
à é
reg
s'ex
la p
doi
ent
que
au
aut
me
per
rel
l'art
levé
git
mer
qu'il
per
obli
diat
la r
con
par
corr
que
lors
l
pas
mon
tion
le m
tion
fichier
cret
tion
vidu
l'inte
L
conc
soc
des

que les données ne seront plus individualisées.

Enfin, l'article 4 précise qu'est interdite sur le territoire belge la collecte de données à caractère personnel dont le traitement n'est pas autorisé en Belgique parce qu'il s'agit de données sensibles et ce, même si les données collectées sont destinées à être traitées en dehors du territoire.

b) Obligation d'information lors du premier enregistrement

L'article 9 prévoit que l'obligation d'information s'exerce lorsqu'une personne est enregistrée pour la première fois dans un traitement déterminé. Elle doit en être immédiatement informée. Que faut-il entendre par "immédiatement" ? Le terme signifie que l'obligation doit être satisfaite simultanément au traitement. Le délai variera donc d'un cas à un autre. Il est certain que le maître d'un grand fichier mettra beaucoup plus de temps à informer les personnes concernées que le maître d'un fichier relativement peu important.

En ce qui concerne l'étendue d'application de l'article 9, une hypothèse intéressante a été soulevée au cours des travaux parlementaires. Il s'agit de l'exemple d'une lettre envoyée à un parlementaire par un électeur potentiel. A supposer qu'il veuille conserver les données à caractère personnel concernant l'auteur de la lettre est-il obligé, en vertu de l'article 9, d'en informer immédiatement son correspondant ? Il a été décidé que la réponse était affirmative. Lorsqu'un fichier est constitué sur base des données communiquées par des personnes qui se sont adressées à leur correspondant par courrier, la loi trouve à s'appliquer.

c) Les exceptions à l'obligation d'information lors du premier enregistrement

L'article 9 prévoit lui-même qu'il ne s'applique pas :

1. lorsque l'information a déjà été donnée au moment de la collecte ;
2. lorsque le traitement se situe dans une relation contractuelle entre la personne concernée et le maître du fichier ;
3. lorsque le traitement se situe dans 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. Cette dernière exception concerne par exemple le fichage d'un individu dans un fichier de la sécurité sociale. Les relations entre les organismes de sécurité sociale et l'intéressé sont régies par la loi.

L'exception la plus délicate est celle qui concerne la relation contractuelle. Ainsi, si une association fait un fichier de ses membres qui sont des sociétés mais indique pour la facilité du

contact le nom des personnes physiques, y a-t-il obligation d'information ? Ne peut-on dire que l'on se situe dans une relation contractuelle ? Tout dépend de la manière dont on entend la notion de relation contractuelle. Si on l'entend au sens strict, il n'existe de relation contractuelle qu'avec la société mais non avec ses dirigeants ou avec ses directeurs.

Il ressort des travaux préparatoires qu'il faut entendre la notion dans un sens large. Le Ministre de la justice a clairement déclaré que l'exception ne concerne pas les relations contractuelles sensu stricto mais vise une notion beaucoup plus large : l'exception s'applique dès que la personne concernée doit raisonnablement se rendre compte que sa demande d'information entraîne l'enregistrement de son nom dans un fichier.

Mais, d'autre part, dès que la relation contractuelle est définitivement terminée et qu'il ne subsiste ni droit ni devoir, le lien est rompu et l'exception ne s'applique plus.

Il est certain que l'interprétation donnée par le Ministre de la justice ne supprime pas tous les problèmes qui peuvent se poser. C'est sans doute pour cette raison qu'il est prévu, dans la loi que le Roi peut, par arrêté délibéré en Conseil des Ministres sur avis de la Commission de la protection de la vie privée, dispenser certaines catégories de traitements de l'application de l'article 9 ou prévoir que certaines catégories de traitements pourront s'y conformer par une procédure d'information collective, dans les conditions et selon les modalités qu'elle détermine.

3. Déclaration préalable et publicité des traitements

L'article 17 dispose qu'avant la mise en oeuvre d'un traitement automatisé de données à caractère personnel le maître du fichier doit faire une déclaration auprès de la Commission de la protection de la vie privée comportant les mentions stipulées à l'article 17 § 3 et notamment l'identité du maître du fichier, la dénomination du traitement automatisé et sa finalité, la période au-delà de laquelle les données ne peuvent plus être gardées, utilisées ou diffusées.

La déclaration vise uniquement les traitements automatisés et non les fichiers manuels.

Pour les traitements à finalités multiples, la déclaration ne doit pas être faite lors de chaque utilisation du traitement. Il suffit d'une déclaration préalable.

Lors de l'accomplissement de la formalité, le maître du fichier devra verser une contribution au comptable institué auprès de la Commission de la

protection de la vie privée. Le montant de cette contribution devrait être de l'ordre de 5 000 FB.

Enfin, le paragraphe 8 de l'article 17 permet au Roi d'exempter d'une déclaration les catégories de traitements automatisés de données à caractère personnel qui ne présentent manifestement pas de risque d'atteinte à la vie privée ou autoriser, pour ces traitements, l'établissement d'une déclaration réduite à certaines mentions.

Il ressort des travaux parlementaires que la détermination des traitements qui bénéficieront des dérogations pourra être inspirée de l'expérience française de la Commission nationale de l'informatique et des libertés (CNIL). Celle-ci dispose en effet d'un pouvoir réglementaire qui lui permet d'établir des normes types, dénommées "normes simplifiées" pour les traitements les plus courants qui ne comportent manifestement pas d'atteinte à la vie privée et aux libertés. Les traitements visés par ces normes simplifiées ne doivent faire l'objet que d'une déclaration de conformité à la norme qui les concerne. Une trentaine de normes simplifiées ont été émises à ce jour. L'on peut citer à titre d'exemple celles concernant la gestion des fichiers de fournisseurs comportant des personnes physiques; les traitements automatisés à des fins statistiques d'informations nominatives se rapportant à des personnes physiques et relatives à leur qualité d'entrepreneurs individuels ou d'aides familiales effectués par les services publics et les organismes d'intérêt public, la gestion des membres des ASBL, la gestion du fichier électoral des communes, ainsi que les traitements relatifs à la facturation de différents services offerts aux parents par les collectivités territoriales (gestion des transports scolaires, restaurants scolaires, garderies, ...).

4. Le fichier des fichiers

L'article 18 de la loi dispose qu'est tenu auprès de la Commission de la protection de la vie privée, un registre des traitements automatisés de données à caractère personnel.

A la suite d'un amendement parlementaire de dernière minute, la loi dispose également que le numéro d'identification du traitement dans le Registre devra figurer sur toute pièce qui en matérialisera l'usage. Un certain nombre de parlementaires estimaient que la personne concernée devait pouvoir en tout temps retracer l'origine de la collecte des données, ce qui impliquait l'indication de la source pour chaque traitement.

Cette exigence légale comporte de sérieux inconvénients :

- d'une part en matière de concurrence, l'in-

sertion du numéro d'identification permettra par exemple aux concurrents des sociétés de marketing direct de déterminer aisément la provenance des adresses pour un type de produits ;

- l'insertion d'un numéro d'identification, outre le fait qu'elle risque de détruire l'impact de personnalisation dans des mailings haut de gamme, va poser de sérieux problèmes pratiques pour les mailings comprenant plusieurs fichiers. Que se passe-t-il en effet lorsqu'une adresse se retrouve dans quatre fichiers différents et qu'elle n'est utilisée qu'une seule fois à la suite d'un procédé dit de "déduplication" ? Faut-il indiquer les quatre numéros d'identification ?

5. Les autres obligations imposées au maître du fichier

Il importe de souligner que les obligations imposées par l'article 16, à l'instar de celles contenues dans l'article 17 ne s'appliquent qu'au maître du fichier, à savoir 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. Elles ne s'imposent pas au gestionnaire du traitement, celui-ci étant défini comme la personne physique ou morale ou l'association de fait à qui est confiée l'organisation et la mise en oeuvre du traitement. Le gestionnaire du traitement est en fait celui qui est chargé d'organiser et de mettre en oeuvre le traitement. Le maître du fichier est celui qui en a la responsabilité.

Les obligations imposées au maître du fichier par l'article 16 sont diverses : obligation d'établir un état pour chaque traitement, de s'assurer de la conformité des programmes avec les termes de la déclaration préalable, de faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes ou non pertinentes, obligation d'assurer la sécurité du traitement.

Celles-ci ont été introduites dans la loi pour satisfaire au prescrit de l'article 7 de la Convention du Conseil de l'Europe qui dispose que "des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès ou la modification ou la diffusion non autorisée".

L'alinéa 3 du paragraphe 3 autorise en outre le Roi à rendre obligatoires des normes générales ou spécifiques pour assurer le respect de ces principes généraux. Cette disposition doit être rapprochée de l'article 45 de la loi qui permet au Roi

de déterminer les autorités qui donneront l'ordre de détruire ou qui seront chargées de la destruction des données en temps de guerre.

Chapitre IV - Le droit des personnes intéressées

La loi donne à toute personne intéressée un droit d'accès et un droit de rectification. Ils sont régis par les articles 10 à 14 de la loi.

1. Le droit d'accès

L'article 10 de la loi donne à toute personne justifiant de son identité - en ce et y compris son représentant légal - le droit d'obtenir communication des données qu'un traitement contient à son sujet. L'article 10 prévoit également que dans la réponse, la personne devra être avertie de la faculté d'exercer les recours prévus aux articles 12 et 14 - c'est-à-dire le droit de rectification et le droit d'agir en référé - et éventuellement de consulter le registre public prévu à l'article 18, c'est-à-dire le fichier des fichiers.

Comment doit procéder l'intéressé ? Il doit adresser une demande datée et signée au maître du fichier ou à toute personne désignée par le Roi. Quels sont les renseignements qui doivent y être communiqués ? Toutes les données que contient le traitement concernant la personne, sans limitation. En effet, le paragraphe 2 de l'article 10 limite le droit d'accès à une demande par délai de 12 mois, étant entendu néanmoins que la Commission de la protection de la vie privée peut, dans des cas exceptionnels, ou lorsqu'a eu lieu une modification des données, imposer le respect d'un délai inférieur.

Dans quels délais doivent être communiquées les données ? Elles doivent être sans délai et au plus tard dans les 45 jours de la réception de la demande. Une redevance préalable pour couvrir les seuls frais administratifs sera fixée par le Roi.

Enfin, en ce qui concerne les données médicales, il est précisé qu'elles seront communiquées à l'intéressé par l'intermédiaire d'un médecin choisi par lui.

D'autre part, aux termes de l'article 11, le droit d'accès ne peut être exercé directement à l'égard des traitements de données à caractère personnel, gérés par des autorités publiques en vue de l'exercice de leurs compétences de police judiciaire, ni à l'égard de traitements de données à caractère personnel gérés par les services de police en vue de l'exercice de leurs compétences de police administrative.

2. Le droit de rectification

L'article 12 de la loi dispose que toute personne a le droit d'obtenir sans frais la rectification de toute donnée à caractère personnel inexacte qui la concerne.

Il précise également que toute personne a le droit d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui compte tenu du but du traitement, est incomplète ou non pertinente et dont l'enregistrement, la communication ou la conservation sont interdits, ou encore qui a été conservée au-delà de la période autorisée.

Il a été indiqué lors de travaux préparatoires que la notion de rectification doit être entendue au sens le plus large. Elle peut consister à supprimer ou à compléter les données erronées ou perçues comme telles. Dans ce dernier cas lorsqu'il s'agit d'une appréciation que comportent les données, la personne concernée n'a pas le droit de la remplacer par sa propre appréciation, mais le maître du fichier devra obligatoirement mentionner que la donnée en question est contestée par la personne à laquelle elle se rapporte.

La Commission de la vie privée avait initialement proposé l'instauration d'un droit de blocage qui eut conduit à ce que les informations ne soient pas communiquées tant que la rectification n'aurait pas été apportée. Il a été jugé qu'une telle règle serait excessive car elle permettrait, dans certaines circonstances, d'entraver considérablement le fonctionnement de la banque de données.

En conséquence, la personne qui estime qu'une donnée la concernant est inexacte - et elle en a bien entendu la charge de la preuve - doit adresser une demande datée et signée au maître du fichier ou à la personne désignée par le Roi. Dans le mois à compter de la demande, le maître du fichier doit communiquer les rectifications ou suppressions de données aux personnes auxquelles les données inexactes, incomplètes ou non pertinentes ont été communiquées pour autant qu'il connaisse encore les destinataires de cette information.

Ce droit de rectification ne s'applique pas aux traitements de données à caractère personnel visés à l'article 11, 2° à 4°, c'est-à-dire les traitements de données à caractère personnel gérés par des autorités publiques en vertu de l'exercice de missions de police judiciaire et administrative. Dans ce cas, le droit d'accès sera exercé par la Commission de la protection de la vie privée, aux termes de l'article 13 de la loi. Aucun délai n'a été prévu pour cet exercice indirect du droit de rectifi-

cation. Par ailleurs, la gratuité est de règle contrairement au principe consacré pour le droit d'accès direct, la gratuité étant d'autant plus souhaitable lorsqu'il s'agit de données pouvant revêtir une importance particulière pour la personne concernée.

3. Absence de droit d'opposition

Contrairement à l'article 15 du projet de Directive européenne, la loi belge ne prévoit pas de droit d'opposition permettant à une personne concernée de refuser qu'un usage soit fait de données la concernant.

L'option du législateur belge s'inscrit dans la philosophie générale de la loi basée sur une conception dite répressive, où tous les traitements sont permis a priori. Accorder le droit d'opposition reviendrait à consacrer un droit de propriété de l'individu sur les données qui le concernent, celui-ci pouvant dès lors empêcher tout traitement pour de simples motifs personnels. Il a donc semblé préférable au législateur de privilégier le respect de la légitimité des finalités, laquelle tiendra compte de la nécessité de respecter la vie privée des personnes tout en intégrant les exigences de la vie en société.

Certes, l'absence de tout droit d'opposition pourra poser des problèmes dans certains cas particuliers. Rien n'empêche cependant que dans certains secteurs soient élaborés des codes d'éthique qui prévoiraient l'existence d'un tel droit d'opposition. L'article 44 de la loi le prévoit en ce qu'il permet au Roi, par arrêté délibéré en Conseil des Ministres, après avis de la Commission pour la protection de la vie privée, de préciser la mise en oeuvre des dispositions contenues dans la loi en vue de tenir compte de la spécificité des différents secteurs. Certains codes d'éthique consacrent le droit d'opposition, ainsi le Code des associations de vente par correspondance : toute personne intéressée peut faire savoir à cette association qu'elle souhaite figurer sur la "Robinson list" et être ainsi radiée d'un fichier déterminé.

Par ailleurs, la loi maintient le jeu de l'article 1382 du Code civil qui permet de mettre en cause la responsabilité d'une personne si les trois éléments constitutifs de la responsabilité quasi délictuelle sont réunis, à savoir la faute, le dommage et le lien de causalité entre la faute et le dommage.

Chapitre V - Les interconnexions et flux transfrontaliers

L'article 21 de la loi prévoit que les rapprochements, interconnexions ou toute autre forme

de mise en relation de données à caractère personnel faisant l'objet de traitements peuvent être, en vue d'assurer le droit au respect de la vie privée, interdits ou réglementés selon les modalités fixées par arrêté royal délibéré en Conseil des Ministres, sur proposition ou après avis de la Commission de la protection de la vie privée.

D'autre part, l'article 22 dispose que, dans le respect des conventions internationales, la transmission entre le territoire belge et l'étranger, sous quelque forme que ce soit, de données à caractère personnel faisant l'objet d'un traitement peut, en vue d'assurer le droit au respect de la vie privée être soit interdite, soit soumise à une autorisation préalable soit être réglementée. L'on vise ici les restrictions éventuelles de transfert de données vers des pays qui n'ont pas de législation en la matière.

Chapitre VI - La commission pour la protection de la vie privée

Elle est régie par les articles 23 à 36.

L'article 23 de la loi crée une Commission pour la protection de la vie privée. L'institution de cette Commission indépendante est évidemment une garantie importante et doit être considérée comme un des piliers des techniques de protection mises en place par le législateur. C'est certainement le cas pour les traitements des données pour lesquels il n'est pas accordé aux intéressés un droit d'accès direct.

Cette Commission est la prolongation de la commission déjà existante qui avait été créée par l'article 12 de la loi du 8 août 1983 sur le Registre national. Elle se voit néanmoins accorder une compétence beaucoup plus large. Par ailleurs, la Commission avait déjà été instituée dans sa nouvelle qualité par l'article 92 de la loi sur la banque Carrefour de la sécurité sociale.

La Commission comporte des membres de droit désignés par les comités de surveillance sectoriels institués par les lois particulières (par exemple, la banque Carrefour de la sécurité sociale) et des membres désignés tantôt par la Chambre, tantôt par le Sénat, parmi lesquels le Président.

Elle a compétence générale de contrôle sur tous les fichiers et traitements de données. Elle dispose par ailleurs de compétences étendues d'avis, de recommandation, de médiation, de plainte, d'examen, de rapport, d'avis préjudiciel, en exécution de dispositions particulières de la loi du 8 décembre 1992 ou d'autres lois particulières. Elle doit également faire rapport au Parlement de son activité.

Chapitre VII - Les sanctions et les voies de recours

1. Les sanctions pénales

Le texte de la loi prévoit dans ses articles 37 à 43 des sanctions pénales. Les peines d'emprisonnement prévues dans le texte initial ont été en général remplacées par des peines d'amendes et de confiscation matérielle qui apparaissent davantage proportionnées au but recherché.

2. Les sanctions civiles

La loi laisse intacte la possibilité de recours sur base de l'article 1382 du Code civil.

3. La compétence du Président du tribunal de première instance siégeant comme en référé.

Aux termes de l'article 14 de la loi, le Président du Tribunal de première instance, siégeant comme en référé, connaît de toutes demandes relatives au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toutes demandes tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée.

L'action prévue à l'article 14, paragraphe 1er, n'est recevable que si la demande d'accès visée à l'article 10, 1er ou la demande de rectification visée à l'article 12, 2 a été rejetée ou s'il n'y a pas été donné suite dans les 45 jours. Le Président du Tribunal pourra donc ordonner l'accès ou la rectification prévue par la loi.

L'article 14 vise également en son paragraphe 6 l'hypothèse où des données inexactes, incomplètes ou non pertinentes ou dont la conservation est interdite, ont été communiquées à des tiers, ou lorsqu'une communication de données a eu lieu après l'expiration de la période durant laquelle la conservation de ces données est autorisée. Dans ce cas, le Président du Tribunal peut ordonner au maître du fichier d'informer les tiers concernés de la rectification ou de la suppression des données.

Enfin, la loi précise que les dispositions des paragraphes 6 et 7 ne limitent en rien la compétence générale dont dispose en la matière le Président du Tribunal de première instance siégeant en référé.

Chapitre VIII - Entrée en vigueur de la loi

L'article 52 dispose que chacune des dispositions de la loi entrera en vigueur à la date fixée par le Roi et au plus tard le 1er jour du 18ème mois suivant le mois de sa publication au Moniteur belge. La loi a été publiée le 18 mars 1993.

L'arrêté royal n° 1 du 28 février 1993 a prévu une entrée en vigueur échelonnée des dispositions de la loi, du 1er août 1993 au 1er septembre 1994.

L'arrêté royal n° 2 de la même date a prévu un délai complémentaire de 3, 6 ou 9 mois selon le cas, pour l'application de différentes dispositions aux fichiers existants.

(*) Article précédemment publié à la *Revue de droit des affaires internationales*, n° 6, 1993, p. 782 s.