La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la Directive 95/46 CE du 24 octobre 1995

Léonard, Thierry; Poullet, Yves

Published in:
Journal des Tribunaux

Publication date:
1999

Document Version
le PDF de l'éditeur

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL EN PLEINE (R)ÉVOLUTION

La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995

I INTRODUCTION

1. — La loi du 11 décembre 1998 publiée au *Moniteur belge* du 3 février 1999 (1) adapte la législation belge, principalement la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, à la directive 95/46/C.E. du 24 octobre 1995 du Parlement européen et 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 (2).

L'article 32 de la directive imposait aux Etats membres d'adopter et de mettre en vigueur, pour le 24 octobre 1998, les dispositions législatives, réglementaires et administratives nécessaires au respect de ses dispositions.

L'adoption de la loi du 11 décembre 1998 représente donc une première étape du processus de transposition (3), qui doit être suivie de la publication des arrêtés d'application de la loi. Par ailleurs, la seconde directive « Protection des données », celle spécifique au secteur des télécommunications (4), attend également une transposition qui n'est actuellement que partiellement réalisée.

La réalisation de cette première étape a suscité peu de débats comme il appert des documents parlementaires (5). Curieusement, l'essentiel des discussions a porté sur les dispositions d'un projet de loi initialement distinct puis réintégré par la suite dans le projet global : le projet de loi n° 1586 relatif à la protection des données à caractère personnel dans le cadre des activités du Centre pour enfants disparus (6).

Les avis respectivement du Conseil d'Etat et de la Commission de protection de la vie privée ont sans doute plus pesé dans les quelques modifications du texte gouvernemental. Voté le 12 novembre 1998 par la Chambre des représentants, le texte ne devait pas être évoqué par le Sénat (7) (8).

---

(1) Loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 févr. 1999, pp. 3049 et s. Cette nouvelle loi intervient par la voie de modification 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. Dans le présent article, toute référence à un article de la « nouvelle loi » vise l'article de la loi de 1992 telle que modifiée par la loi du 11 décembre 1998.

(2) *J.O.C.E.*, L 281/31, 23 nov. 1995. Pour un commentaire des directives européennes en matière de protection des données, lire S. Louveaux, Y. Poullet, V. Willems, *A Business Guide to changes in European Data Protection Legislation*, Cullen Intern. (ed.), Kluwer Law Int., 1999.

(3) On soulignera que la Belgique est loin d'être le mauvais élève de la classe européenne en la matière. Seuls l'Italie, la Grèce, le Portugal, la Suède et le Royaume-Uni ont déjà adopté une législation conforme à la directive.

(4) Directive 97/66/C.E. du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *J.O.C.E.*, L 24/1, 30 janv. 1998.

(5) Pour être précis, quatre réunions de la Commission de la justice les 9 et 23 juin, les 1er et 7 juillet 1998.

(6) Projet de loi n° 1586/1. Ce projet de loi fut réuni au projet global lors de la réunion du 7 juillet 1998 de la Commission de la justice. Il ne s'agit pas ici de minimiser l'importance de ce centre mais bien de relever la disproportion entre le temps qui lui a été consacré et celui dont a bénéficié l'essentiel des modifications du régime de protection.

(7) Ce qui est à proprement parler incompréhensible. Le Sénat se doit d'intervenir dans les débats de fond relatifs aux libertés et droits fondamentaux comme en l'espèce.

(8) Les abréviations suivantes renvoient aux documents suivants :
Exposé des motifs: Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1; Avis du Conseil d'Etat : Avis rendu par le Conseil d'Etat le 2 févr. 1998, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1; Rapport: Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. ord.

Il revient au Roi de fixer la date d'entrée en vigueur de chaque disposition de la nouvelle loi. Il est également chargé de fixer le délai dans lequel le responsable du traitement doit se conformer aux dispositions légales concernant les traitements existant au moment de leur entrée en vigueur (9) (10).

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

2. — Le champ d'application matériel et personnel de la loi du 8 décembre 1992 dépend des définitions données aux concepts clés de la protection. D'importants changements sont insérés par la nouvelle loi.

Les premiers sont d'ordre terminologique. Le « maître du fichier » devient le « responsable du traitement ». Le concept ambigu de « gestionnaire du traitement » est remplacé par celui de « sous-traitant ». La notion de « tenue d'un fichier manuel » disparaît. Les seconds touchent au fond. Toutes les définitions contenues dans l'ancienne loi sont modifiées. De nouvelles définitions font leur apparition à la suite de la directive. Elles portent sur les concept de « tiers », de « destinataire » et de « consentement de la personne concernée ».

Enfin, le champ d'application — tant matériel que territorial — de la loi du 8 décembre 1992 est largement modifié.

1.1. — Les définitions modifiées

3. — Le concept de « donnée à caractère personnel » fait l'objet d'une importante précision (11). S'il s'agit toujours de « toute information concernant une personne physique identifiée ou identifiable », la nouvelle loi, reprenant textuellement la directive, répute comme 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 ».

Un numéro de téléphone, de plaque d'immatriculation de voiture, de sécurité sociale ou de passeport peut ainsi être considéré comme une donnée à caractère personnelle (12).

La précision apportée par la directive posait une difficulté importante quant à la détermination des données « anonymes » ou « non identifiables » (13). Le considérant n° 26 de la directive indiquait que « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne » (14). Une interprétation raisonnable de ce considérant permettait d'admettre comme anonymes des données pour lesquelles le responsable du traitement ne disposait pas des moyens techniques suffisants pour opérer l'identification — et offrait des garanties spécifiques quant à l'absence de recherche d'identification — bien que la possibilité existe techniquement *in abstracto* soit dans son chef, soit dans le chef d'un tiers.

L'exposé des motifs de la nouvelle loi rejette clairement cette interprétation (15). Dès lors qu'il existe un moyen raisonnable d'identifier les personnes concernées, soit dans le chef du responsable du traitement, soit même par un tiers, il s'agit d'une donnée à caractère personnel dont le traitement est susceptible d'être réglementé par la loi. Il reviendra à la jurisprudence de trancher définitivement cette question dont les effets pratiques ne doivent pas être sous-estimés (16).

4. — La notion de « traitement » est également sensiblement modifiée. Le système antérieur, qui distinguait le « traitement automatisé » de la « tenue d'un fichier manuel », a vécu. Dorénavant, le traitement vise indistinctement « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel » (17).

Ce faisant, le concept voit son champ d'application élargi. Le catalogue des opérations qualifiables de traitement s'est sensiblement enrichi. La collecte, absente de l'ancienne définition, en fait maintenant partie intégrante. Le traitement existe, que des procédés automatisés soient ou non utilisés.

Peu importe également qu'une seule opération soit effectuée sur les données à caractère personnel. Cette extension de la notion de traitement entraîne un élargissement du champ d'application de la loi. Ainsi, la simple consultation d'une banque de données en ligne ou d'une page Web sur l'Internet pourrait bien impliquer son application intégrale dans le chef du consultant (18). Cette conception a déjà été amplement critiquée (19). Quel est en effet le sens à donner à l'obligation d'informer la personne concernée ou à l'obligation de notification auprès de la Commission de la protection de la vie privée si les données consultées ne font l'objet d'aucune conservation ou enregistrement dans le chef du consultant? (20)

1998-1999, n° 1566/10; Avis : Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 1566/10. La protection des données à caractère personnel en droit communautaire : M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau, Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, pp. 121 à 127, pp. 145 à 155, et pp. 173 à 179.

(9) Article 52 de la nouvelle loi.

(10) Le présent commentaire tente de privilégier l'aspect critique et analytique des modifications apportées au texte de l'ancienne loi du 8 décembre 1992. On n'y trouvera donc pas un exposé systématique de la protection telle qu'elle découle du texte modifié et des interprétations doctrinales et jurisprudentielles du texte ancien de la loi. Sur le projet de loi déposé à la chambre, voy. F. De Brouwer et S. Louveaux, « Protection des données à caractère personnel : vers une nouvelle loi belge », *Rev. Ubiquité*, 1998, pp. 83 à 99.

(11) Article 1er, §1er, de la nouvelle loi.

(12) Les traitements dits « invisibles » sur l'Internet risquent également d'être largement soumis à la loi dès lors que le moyen d'identification utilisé est relié directement ou indirectement au nom de « l'internaute ». Une évolution de la notion d'identité sur le réseau des réseaux s'impose toutefois si l'on ne veut pas voir rejeter ces traitements du champ d'application de la loi dès lors qu'aucun lien n'est opéré entre le moyen d'identification (par exemple un cookie) et le nom de la personne (voy. sur ce point J.-M. Dinant, *Les traitements invisibles sur l'Internet*, disponible à l'adresse http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html; « L'électronisation du commerce », *Rev. gén.*, 1999/3, pp. 39 et s.).

(13) La protection des données à caractère personnel en droit communautaire, pp. 124 et 125, nos 12 et 13.

(14) Il ajoutait en outre que la protection n'était pas accordée aux données rendues anonymes, d'une manière telle que la personne concernée n'est plus identifiable.

(15) Exposé des motifs, p. 12, notam. : « Une information relative à une personne est donc considérée comme donnée à caractère personnel tant que quelqu'un est encore en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme "données à caractère personnel" les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne ». La Commission de la protection de la vie privée avait opté pour une position plus nuancée considérant que « il n'est question, dans ce cas, d'un traitement de données à caractère personnel dans le chef du responsable du traitement que dans la mesure où il dispose de la possibilité pouvant être raisonnablement mise en œuvre de pouvoir procéder à un décodage via le tiers », Avis, p. 113.

(16) Ainsi par exemple, des données « codées » en matière de sécurité sociale ou de recherches scientifiques tomberont sous le champ d'application de la loi dès lors qu'un moyen raisonnable existe de les réidentifier.

(17) Article 1er, § 2 de la nouvelle loi.

(18) Exposé des motifs, p. 13 : « Une extraction, par exemple, ou une consultation unique d'un fichier contenant des données à caractère personnel constitue également un traitement auquel s'appliquent les dispositions de la loi »; pour autant que cette opération unique tombe sous le champ d'application territorial de la loi.

(19) La protection des données à caractère personnel en droit communautaire, pp. 125 et 126, n° 16; M.-H. Boulanger, C. de Terwangne, « Internet et le respect de la vie privée », *in Internet face au droit*, Diegem-Namur, Story Scientia-C.R.I.D., *Cahiers du C.R.I.D.*, n° 12, 1997, pp. 198 et 199.

(20) Le ministre paraît s'être rendu compte de la difficulté. Il fait dès lors la distinction entre les principes de base de la loi — principe de finalité et de qualité des données — applicables même à une seule opération, et les autres obligations de la loi, telle l'obligation d'information ou de notification, qui ne devraient pas forcément être respectées. Ainsi, l'obligation d'information en cas de collecte auprès d'une personne autre que la personne concernée (art. 9, § 2 nouv.) ne s'applique qu'en cas d'enregistrement ou de communication des données à des tiers. En outre, l'obligation de déclaration ne devrait pas être exécutée dès lors que l'article 17, § 1er nou-

La (ou les) finalité(s) d'utilisation des données révèle(ent) l'élément unificateur du traitement, sans qu'une condition de structuration *a priori* des informations s'impose. Contrairement à la situation antérieure, un traitement peut viser différentes finalités d'utilisation (21). Toutes ces finalités peuvent-elles être visées par un seul et même traitement? La réponse doit être négative. On verra que les finalités du traitement doivent être « compatibles » (22) en vertu du principe de finalité et que seul un ensemble de « finalités liées » (23) peuvent faire l'objet d'une seule déclaration. Ce faisant, le concept perd de sa cohérence. Il devient plus difficile de distinguer *a priori* les différents traitements de traitement entre eux. On peut craindre également que les personnes concernées soient mises dans l'impossibilité de contrôler les données et traitements qui les concernent dès lors qu'ils ne seraient plus capables de déterminer sur quelles données porte chacune des finalités du traitement.

5. — La notion de « fichier » a également été modifiée (24). Le but est toujours d'exclure du champ d'application de la loi les dossiers non automatisés. Le critère retenu est précisé par rapport à l'ancienne loi. La structure des données à caractère personnel doit permettre leur accessibilité selon des critères déterminés. Ce ne sont donc pas les dossiers (25) eux-mêmes qui doivent faire l'objet d'une organisation ou structuration mais bien les données qu'ils contiennent. La nouvelle loi est cependant muette concernant le niveau d'accessibilité à atteindre pour admettre la qualification de fichier. On peut donc s'attendre à ce que la controverse continue sur ce point (26).

6. — Les concepts de « maître du fichier » et de « gestionnaire du traitement » ont été remplacés par les définitions de « responsable du traitement » et de « sous-traitant ».

Le responsable du traitement, destinataire de la plupart des obligations légales, voit sa définition modifiée sur deux points (27).

Si le critère de la détermination des finalités est conservé, celui de la détermination des « moyens » du traitement remplace celui du choix des catégories de données, présent dans l'ancienne loi. Les deux critères sont dorénavant cumulatifs, ce qui n'ira pas sans poser des difficultés lorsque la finalité sera ainsi déterminée par la maison mère d'une société établie dans un pays tiers, et les moyens par la filiale belge (28).

La définition légale indique que la prise de décision quant aux finalités et moyens du traitement peut être conjointe, ce qui impliquera alors l'identification de plusieurs responsables à l'égard d'un même traitement (29). Ainsi, si différents opérateurs de télécommunication centralisent des données relatives aux abonnés présentant des retards de payement, ils seront chacun considérés comme responsable du traitement centralisé. Par contre, s'ils se groupent en une entité juridique distincte, cette dernière apparaîtra comme le responsable des divers traitements de données créés en son sein. On peut notamment penser aux centrales de crédit ou de risques particuliers en matière d'assurance.

Celui qui traite les données pour le compte du responsable est désigné par le terme de « sous-traitant » (30). Il peut s'agir du prestataire informatique qui gère le traitement, de l'entreprise de marketing direct qui met à jour les données de ses clients, du secrétariat social qui gère le paiement des salaires pour une p.m.e. (31), etc. Il est précisé que le sous-traitant doit être distingué de celui qui traite les données sous l'autorité directe du responsable, à savoir principalement le préposé ou le fonctionnaire agissant dans le cadre de leur contrat de travail ou statut.

7. — La loi nouvelle introduit trois nouveaux concepts, conformément à la directive.

La notion de « tiers » (32) n'est pas totalement nouvelle puisqu'elle se retrouvait *mutatis mutandis* déjà dans l'arrêté royal n° 13 du 12 mars 1996 prévoyant certaines exceptions à l'obligation de déclaration. Elle permet notamment de mieux appréhender les cas de communication aux tiers conditionnant bon nombre de dispositions de la loi ou de ses arrêtés royaux d'application. Il s'agit de toute autre personne que le responsable du traitement, le sous-traitant et les personnes qui traitent les données sous leur autorité directe.

Le concept de « destinataire » fait par contre son apparition (33). Proche de la notion de « tiers » en ce qu'il vise les personnes qui reçoivent communication des données, il s'en distingue cependant par le fait que ces personnes peuvent faire partie de l'entité du responsable du traitement ou du sous-traitant. On vise donc par là, outre la communication à des tiers au sens précité, les flux d'informations entre départements d'une même société ou administration (34). Cette notion est principalement utilisée dans le cadre de l'obligation d'information qui impose notamment au responsable du traitement d'informer la personne concernée des destinataires de données.

La loi définit enfin ce qu'il faut entendre par le « consentement de la personne concernée ». On verra que le consentement de la personne concernée joue un rôle essentiel dans la protection mise en place. Il permet dans certaines conditions de légitimer un traitement ou de lever l'interdiction de traitement des données sensibles. La loi vise par là « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données (...) à caractère personnel la concernant fassent l'objet d'un traitement » (35).

Toute manifestation de volonté peut constituer un consentement. Il ne doit pas nécessairement être donné par écrit et peut être

veau ne vise qu'un traitement ou un ensemble de traitements ayant une même finalité ou un ensemble de finalités liées (Exposé des motifs, p. 13). On admet ne pas être convaincu. Même si le raisonnement est correct concernant l'article 9, § 2, il tombe concernant l'information lors de la collecte auprès de la personne concernée par les données (art. 9, § 1er, nouv.). En outre, même si différentes finalités liées peuvent donner lieu à une même déclaration, un seul traitement dans le chef par exemple du consultant, implique également l'obligation de déclaration sauf exception légale ou réglementaire.

(21) Voy. *infra*, tant la définition du responsable du traitement (art. 1er, § 4, de la nouvelle loi), que l'obligation d'information (art. 9, § 1er, *c*, et 9, § 2, *b*, de la nouvelle loi), que le droit d'accès (art. 10, § 1er, *a*, de la nouvelle loi) visent « les finalités du traitement ». L'obligation de déclaration admet également qu'un ensemble de finalités liées correspondant à un traitement (art. 17, § 3, 5°, de la nouvelle loi).

(22) Voy. *infra*, n° 29.

(23) Voy. *infra*, n° 60.

(24) Article 1er, § 3, de la nouvelle loi : « tout ensemble de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

(25) Le considérant 27 de la directive précise bien que « les dossiers ou ensemble de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés n'entrent en aucun cas dans le champ d'application de la présente directive ».

(26) Il est significatif que la seule affaire belge ayant donné lieu, en la matière, à un arrêt de la Cour de cassation ait précisément porté sur la définition du « fichier » (voy. Cass, 1re ch., 16 mai 1997, *J.T.*, 1997, p. 779). Sur l'arrêt entrepris, voy. Anvers, 1re ch., 27 sept. 1995, *A.J.T.*, 1995-96, note J. Dumortier; *R.W.*, 1995-1996, p. 750. Pour une critique de cet arrêt, voy. Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *in Guide juridique de l'entreprise*, 2e éd., tit. XI, liv. 112, Diegem, Kluwer, 20 déc. 1996, p. 15, n° 130.

(27) Article 1er, § 4, de la nouvelle loi : « la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance ».

(28) On reste persuadé que le seul critère de la finalité eût suffit (voy. M.-H. Boulanger, C. de Terwangne et Th. Léonard, « La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel », *J.T.*, 1993, p. 373, n° 16). Le ministre précise d'ailleurs que l'important est de désigner comme responsable du traitement, celui qui dispose du pouvoir de décision sur sa finalité (Exposé des motifs, p. 15).

(29) Exposé des motifs, p. 15.

(30) Article 1er, § 5, de la nouvelle loi : « la personne physique ou morale, l'association de fait ou l'administration publique, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ».

(31) Il faudra cependant ici tenir compte de toutes les circonstances de fait. Voy. pour une analyse plus nuancée, Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *op. cit.*, p. 17, n° 180.

(32) Article 1er, § 6, de la nouvelle loi : « la personne physique, la personne morale, l'association de fait ou l'administration publique, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données ».

(33) Article 1er, § 7, de la nouvelle loi : « la personne physique, la personne morale, l'association de fait ou l'administration publique qui reçoit communication de données, qu'il s'agisse ou non d'un tiers (...) »; cette disposition précise en outre que « les instances administratives ou judiciaires qui sont susceptibles de recevoir communication de données dans le cadre d'une enquête particulière ne sont toutefois pas considérées comme des destinataires ».

(34) Exposé des motifs, p. 16.

(35) Article 1er, § 8, de la nouvelle loi.

implicite, sauf exception prévue par la loi (36).

Le consentement doit être libre c'est-à-dire être donné en dehors de toute pression. L'idée est de prévenir toute menace de discrimination suite au choix de la personne concernée. Cette condition paraît bien illusoire en pratique. La pression économique consistant dans le risque de se voir refuser un produit ou un service considérés à tort ou à raison comme essentiels par la personne concernée l'amènera bien souvent à donner son consentement sans aucun esprit critique.

Le consentement doit également être spécifique. Il ne peut avoir un objet général mais doit porter sur des traitements précisément définis notamment en leurs finalités, poursuivis par des responsables déterminés.

Le consentement doit enfin être informé. Le responsable du traitement doit donc transmettre à la personne concernée toute information nécessaire à l'analyse du risque particulier que représente le traitement envisagé pour ses droits et libertés. A cet égard, l'information reçue conformément à la loi (36*bis*) par la personne concernée au moment de la collecte semble constituer un minimum.

1.2. — Le champ d'application matériel et personnel

8. — Le nouvel article 2 énonce le fondement de l'intervention législative : « Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée ».

Ce faisant, la nouvelle loi élargit sensiblement le fondement de la protection. Il ne s'agit plus seulement, comme l'indiquait auparavant cette disposition, de protéger la vie privée des individus. C'est en effet l'ensemble des libertés et droits fondamentaux des personnes physiques qui peuvent être énervés lors de traitements de données à caractère personnel. On retrouve ici l'idée d'un élargissement de la protection traditionnelle en matière de protection de la vie privée (37). *A priori*, aucune distinction n'est à opérer suivant le caractère public ou privé de l'information : tout traitement de données à caractère personnel tombe sous le champ d'application de la protection qu'il révèle ou non une ingérence dans la vie privée de l'individu (38).

En ce qui concerne la protection de la vie privée des individus, le texte protecteur doit cependant être éclairé et interprété par référence à l'article 8 de la Convention européenne des droits de l'homme et à l'article 22 de la Constitution (39).

9. — L'article 3, § 1er, précise que la loi s'applique à tout traitement de données à caractère personnel, qu'il soit automatisé en tout ou en partie, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Sur le fond, la situation antérieure n'est donc pas modifiée. Seul le vocabulaire a changé. Dès lors que la loi vise dans ses dispositions tout traitement, sans précision, ces dernières s'appliquent tant aux traitements automatisés qu'aux traitements non automatisés contenues dans un fichier. Plusieurs de ses dispositions ne viseront cependant que les traitements automatisés.

Concernant les personnes morales, la loi n'est en rien modifiée : elles sont exclues de la protection légale. Seules les personnes physiques jouissent du système protecteur.

Différentes exceptions totales ou partielles au champ d'application sont prévues par les paragraphes 2 à 5 de la nouvelle loi. Certaines étaient déjà prévues par l'ancienne loi (40). Seules les exceptions nouvelles feront l'objet d'un commentaire ci-après.

1.2.1. — *Les exceptions au bénéfice des traitements à finalité journalistique ou d'expression littéraire ou artistique*

10. — L'article 3, § 3, de la nouvelle loi prévoit quatre catégories d'exceptions concernant les « traitements de données à caractère personnel effectuées aux seules fins de journalisme ou d'expression artistique ou littéraire ». Le but était ici de se conformer à l'article 9 de la directive qui imposait aux Etats membres de prévoir des exemptions et dérogations aux principes fondamentaux de la protection « dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression ».

Cette disposition justifierait à elle seule un commentaire exhaustif et approfondi. C'est d'autant plus vrai que son introduction a provoqué un réel débat lors des travaux à la Chambre et, auparavant, au Conseil d'Etat. Le cadre forcément général de la présente étude impose cependant de se limiter à une simple présentation du système mis en place.

11. — L'ancienne loi ne prévoyait aucune exception en faveur des traitements poursuivis par la presse ce qui n'allait pas sans poser certaines difficultés, du moins en théorie (41) (42).

Le principe reste la soumission des journalistes et de leurs traitements au régime protecteur. Certaines dispositions de la nouvelle loi recevront cependant exception dans les conditions strictement énoncées par la loi.

La condition essentielle concerne la finalité du traitement qui doit viser les « seules fins de journalisme ou d'expression artistique ou littéraire ». Malgré la demande expresse du Conseil d'Etat (43), la loi n'apporte pas de précision sur ce qu'il faut entendre par « finalité de journalisme » ou « finalité d'expression artistique ou littéraire » (44). Faut-il dans le premier cas être en possession d'une carte de journaliste ou tout individu diffusant de l'information au nom de sa liberté d'expression, par exemple en éditant des « news » sur l'Internet, peut-il se prévaloir de l'exception? Toute œuvre protégée par le droit d'auteur révélant un traitement de données à caractère personnel bénéficie-t-elle de l'exception ou suffit-il que le caractère artistique — mais comment le définir? — soit présent? Ni le législateur belge, ni le législateur européen ne répondent très clairement à ces questions. Une approche purement fonctionnelle paraît de-

(36) Par exemple en matière de données dites sensibles (cf. *infra*, n° 37).

(36*bis*) Cf. *infra*, n° 44.

(37) Voy. sur ce point, Th. Léonard, observations sous Civ. Bruxelles, prés., 22 mars 1994, *J.T.*, 1994, pp. 849 et 850.

(38) Il est à noter, que les anciennes exceptions au champ d'application de la loi, prévues aux anciens articles 3, § 2, 2° et 3°, et fondées sur la publicité antérieure des données ordonnée par la loi ou un règlement, ou demandée par la personne concernée ont disparu. Voy. cependant l'importante exception au bénéfice des finalités de journalisme ou d'expression artistique ou littéraire, *infra*, n° 12.

(39) La protection des données à caractère personnel en droit communautaire, p. 146, n° 29.

(40) Ainsi, en est-il des traitements de données à caractère personnel effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques (art. 3, § 2, de la nouvelle loi) et des traitements rendus nécessaires par la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins de blanchiment de capitaux (art. 3, § 5, 4°, de la nouvelle loi).

(41) Pour une réflexion plus approfondie, voy. M. Flamée, Th. Léonard, « La liberté de la presse à l'aune de la protection des données : liberté responsable ou liberté surveillée? », *R.G.D.C.*, 1997, pp. 5 à 42; voy. aussi Avis n° 09/95 du 5 avril 1995 de la Commission de la protection de la vie privée concernant l'application 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 par les médias (cet avis n'a pas été publié mais a fait l'objet d'un commentaire *in* Commission de la protection de la vie privée, *Rapport d'activité 1994-1995*, pp. 19 et 20). *Adde*, Recommandation du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, « Législation sur la protection des données et médias », n° 1/97, 25 févr. 1997, Commission européenne, DG XV, 5012/97-FR (http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm).

(42) Il faut dire que l'application de ce type de législation à la presse reste souvent peu compréhensible pour tout un chacun. Il est dès lors utile de rappeler que des traitements de données à caractère personnel peuvent apparaître à chaque niveau de préparation des articles ou émissions de presse : collecte des informations et le cas échéant numérisation et enregistrement de celles-ci, insertion dans des banques de données rédactionnelles et utilisation de celles-ci, utilisation de traitements de texte, de logiciels de mises en page, publication des informations, etc. En bref, « Tout le traitement de l'information effectué par le journaliste et son organe de presse est donc susceptible d'être visé par le champ d'application de la loi » (M. Flamée et Th. Léonard, « La liberté de la presse à l'aune de la protection des données : liberté responsable ou liberté surveillée? », *op. cit.*, p. 14); voy. également dans le même sens, *mutatis mutandis*, la déclaration du ministre concernant la publication d'une décision judiciaire par le biais de l'Internet, pour laquelle un intervenant considérait qu'il n'y avait pas de traitement au sens usuel du terme : « Le ministre confirme qu'il s'agit effectivement, dans l'exemple cité, d'un traitement. Pourraient, en l'occurrence, être considérées comme un traitement, l'organisation, la conservation, éventuellement la modification si le texte est pourvu d'un titre, la transmission et la diffusion (*n.d.l.r.* : du texte) » (Rapport, p. 73).

(43) Avis du Conseil d'Etat, pp. 186 à 188.

(44) L'exposé des motifs vise les traitements opérés par les « journalistes », « artistes » et « écrivains » et renonce explicitement à tout essai de définition des notions employées « parce que l'interprétation de ces notions, issues d'une directive européenne, relèvent en dernier ressort de la compétence de la Cour de justice » (Exposé des motifs, pp. 18 et 19; *adde*, p. 11), ce qui n'est pas sans créer dans l'attente de cette décision, une large incertitude.

voir être privilégiée. La loi vise à réglementer la finalité des traitements, non certaines catégories professionnelles ou des œuvres particulières (45). Il s'agit d'exempter certains traitements dont la finalité est la production en vue de la communication au public d'une expression dont la prétention esthétique, intellectuelle ou d'information sur l'actualité est affirmée. A ce propos, le responsable du traitement ne sera pas forcément un journaliste, un écrivain ou un artiste mais l'organe de presse, l'éditeur, etc.

12. — La première exception concerne le traitement des données dites « sensibles » visées par les articles 6, 7 et 8 de la loi (46). On y retrouve notamment les données relatives aux opinions politiques, à l'appartenance syndicale, les données judiciaires et les données médicales.

Ces données pourront être traitées aux seules fins de journalisme ou d'expression artistique ou littéraire à condition que « le traitement se rapporte à des données rendues manifestement publiques par la personne concernée ou sur des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée » (47).

Cette disposition exprime un retournement du principe de protection retenu par ailleurs dans la loi. Le principe n'est plus ici l'interdiction de traitement des données « sensibles » prévue aux articles 6, 7 et 8 de la loi. Au contraire, la liberté de traitement est proclamée si le responsable croit pouvoir s'autoriser d'une des trois situations prévues dans la disposition (48).

13. — La seconde exception concerne l'obligation d'information contenue dans l'article 9 de la nouvelle loi (49). Soit la collecte de l'information s'effectue auprès de la personne concernée par les données : le responsable du traitement aux seules fins de journalisme ou d'expression artistique ou littéraire est exonéré de l'obligation « lorsque son application (n.d.l.r. : de l'article 9, § 1er) compromettrait la collecte des données auprès de la personne concernée par les données ». Soit les données à caractère personnel sont obtenues auprès d'autres personnes que celle concernée par les données : l'obligation prévue à l'article 9, § 2, disparaît si son application soit compromet la collecte des données ou une publication en projet, soit fournit des indications sur les sources d'information.

La troisième exception concerne l'application des articles 10 et 12 relatifs respectivement aux droits d'accès et de rectification des données (50). On retrouve ici deux des conditions prévues pour l'exception d'information. L'application de ces dispositions ne reçoit exception que si elle compromettrait une publication en projet ou fournirait des indications sur les sources d'information.

La quatrième exception est inconditionnée (51). Pour autant qu'il soit soumis à l'obligation de déclaration, le responsable d'un traitement à finalité « journalistique » ou « artistique » ne devra pas indiquer à la Commission de la protection de la vie privée ni les modalités prévues pour l'information de la personne concernée et l'exercice de ses droits d'accès et de rectification ni les motifs sur lesquels il fonde l'application à son bénéfice de la disposition commentée. Ces traitements ne seront pas repris dans le registre des traitements automatisés tenu par la Commission. Enfin, les dispositions relatives aux flux transfrontières ne s'appliquent pas aux traitements commentés.

14. — En conclusion sur la problématique délicate de l'application de la loi au secteur de la presse, on se limitera à deux réflexions.

Le système mis en place par la nouvelle loi reporte sur les épaules du seul journaliste le soin d'effectuer une pondération plus que délicate entre la liberté d'expression ou le droit légitime à l'information du public et la nécessaire protection des droits et libertés individuelles des personnes concernées par les données. Si le journaliste se trompe *a priori*, il risque d'être passible de sanctions civiles et pénales susceptibles de s'appliquer en cas de violation de la loi. Il sera bien seul et désarmé, tiraillé entre des intérêts contradictoires, et pressé par des impératifs économiques de vente auprès d'un public souvent trop friand de l'étalage de la vie privée d'autrui. La nouvelle loi donnait l'occasion de réfléchir à la mise en place d'un organe neutre, émanant de ce secteur mais composé également de spécialistes de la protection recherchée, ayant comme fonction d'aider le journaliste dans ses choix et de réfléchir à la conciliation des libertés et droits en opposition. La Commission de la protection de la vie privée, tournée nécessairement vers la défense des seuls intérêts individuels, ne présente en effet pas les conditions de neutralité suffisantes pour jouer ce rôle.

Le débat tenu à la Chambre, s'il a eu au moins l'avantage d'exister, n'a pas été suffisant. De trop nombreux points restent dans l'ombre. On regrette que les débats n'aient porté que sur l'application de la loi au secteur de la presse écrite, sans réflexion sur ses implications sur le secteur de l'audiovisuel ou de la presse électronique devenue réalité sur l'Internet. Ensuite, l'application des dispositions non visées dans les exceptions risquent également de poser une foule de problèmes qu'il était pourtant aisé de prévoir (52).

1.2.2. — *Les autres exceptions au champ d'application matériel*

15. — Comme sous l'ancienne loi, une exception est prévue à l'article 3, § 4, de la nouvelle loi concernant les traitements de données à caractère personnel à finalités de sécurité publique (53). Le champ d'application de la disposition est cependant étendu. Il vise aujourd'hui les traitements gérés par la sûreté de l'Etat, par le service général du renseignement et de la sécurité des Forces armées, par l'autorité de sécurité, par les officiers de sécurité et par le comité permanent de contrôle des services de renseignement et d'enquête. Il faut néanmoins que ces traitements soient nécessaires aux missions des services visés.

Ces autorités sont exemptées de la presque intégralité des dispositions de la loi. Ainsi, ne sont pas applicables : le régime d'interdiction des données sensibles prévu aux articles 6 à 8 de la nouvelle loi; l'obligation d'information de la personne concernée, les articles 10 et 12 relatifs aux droits d'accès, de rectification et d'opposition (54); l'action en cessation organisée par l'article 14, l'obligation de notification auprès de la Commission de la protection de la vie privée (55) et la possibilité d'être mis en cause auprès de celle-ci à la suite d'une plainte d'un particulier prévue à l'article 31, §§ 1er à 3, ainsi que la possibilité de réglementation par arrêtés royaux, prévue à l'article 17*bis*, alinéa 1er.

Par contre, les dispositions relatives à la qualité des données et à la licéité des traitements (56) restent d'application. Ce reliquat de protection risque cependant d'être bien illusoire (57).

(45) Pour le ministre, les personnes « pratiquant le journalisme occasionnel » sont également visées, en plus des journalistes professionnels. Ce serait donc bien un critère fonctionnel qu'il faudrait privilégier (Rapport, pp. 77 et 80 : « [...] la personne qui écrit un seul article et collecte des données à cet effet relèvera du champ d'application de la disposition »). Cette approche paraît également privilégiée par un membre de la Commission de la justice qui déclare « [...] ces dispositions concernent la finalité du traitement et non le statut du responsable ni l'œuvre produite. Le droit à la vie privée et la liberté d'expression sont reconnus à tous les citoyens. Les journalistes n'ayant pas le monopole de la liberté d'expression, il n'est donc pas non plus nécessaire d'appartenir à cette catégorie professionnelle pour pouvoir réunir des données en vue de leur publication. La finalité est primordiale et c'est sur ce point que le juge devra se prononcer en cas de conflit » (*idem*, p. 78).

(46) Cf. *infra*, nos 34 et s.

(47) Article 3, § 3, *a*, de la nouvelle loi.

(48) Cette liberté de traitement est cependant loin d'être entière. Outre les règles traditionnelles de droit commun relevant principalement de la responsabilité civile, d'autres obligations issues de la loi commentée trouvent à s'appliquer. Ainsi, le responsable du traitement de données sensibles sera soumis au principe de finalité et de qualité des données inscrit à l'article 4 de la nouvelle loi. Les données devront être traitées loyalement et licitement, elles ne pourront être collectées que pour des finalités déterminées, explicites et légitimes, elles devront être adéquates, pertinentes et non excessives au regard de la finalité et seront soumises au principe d'exactitude. Autant de règles susceptibles de brider plus ou moins largement la liberté d'expression ou le célèbre « droit à l'information » dont se prévalent, à tort ou à raison, les médias pour justifier toute atteinte aux droits et libertés individuels. D'autres règles, qui ne reçoivent pas exception, pourraient du reste s'avérer particulièrement utiles pour la protection de l'individu mais également donner lieu à des interprétations pour le moins délicates : la finalité « journalistique » ou « artistique » devra être légitimée par une des circonstances prévues au nouvel article 5 de la loi et la personne concernée par les données pourra saisir le président du tribunal de première instance, dans les conditions prévues à l'article 14 de la loi.

(49) Article 3, § 3, *b*, de la nouvelle loi.

(50) Article 3, § 3, *c*, de la nouvelle loi.

(51) Article 3, § 3, *d*, de la nouvelle loi.

(52) Voy *supra*, note 49.

(53) Pour une critique approfondie du système introduit par la nouvelle loi, voy. Y. Poullet et B. Havelange, « Secrets d'Etat et vie privée : ou comment concilier l'inconciliable? », colloque organisé par le Comité R. le 20 janvier 1998, *Secret d'Etat ou transparence*, Bruxelles, en cours de publication, n° 15.

(54) Ces droits peuvent s'exercer « indirectement » auprès de la Commission de la protection de la vie privée en application de l'article 13 de la nouvelle loi.

(55) Et par voie de conséquence, l'article 18 qui prévoit la tenue du registre public des traitements automatisés.

(56) Articles 4 et 5 de la nouvelle loi.

(57) Comment intenter, une action judiciaire contre ces autorités sans savoir quelles données sont trai-

Etrangement, cette exception n'a fait l'objet d'aucun débat parlementaire alors qu'elle ouvre et élargit une brèche importante dans la protection des droits individuels des citoyens (58). Du reste, ni le Conseil d'Etat ni la Commission de la protection de la vie privée n'y ont consacré des développements dans leurs avis respectifs. Encore un débat manqué?

16. — L'article 3, § 5, de la nouvelle loi prévoit également toute une série d'exceptions aux droits à l'information ainsi qu'aux droits d'accès et de rectification de la personne concernée. Il s'agit généralement des traitements tenus par des autorités publiques — principalement des services de police (59) — en vue de leurs missions de police judiciaire et administrative.

Si ces exceptions peuvent paraître justifiées dans un certain nombre d'hypothèses, leur généralisation inquiète. S'il est vrai que les personnes concernées se voient reconnaître un droit d'accès et de rectification « indirect » par le biais de la Commission de la protection de la vie privée (60), il n'en reste pas moins que ce droit sera souvent dénué d'objet, la personne n'étant pas informée des données traitées à son sujet.

17. — La dernière exception est celle qui aura donné lieu aux débats les plus importants à la Chambre. Elle bénéficie au très médiatique (61) « Centre européen pour enfants disparus et sexuellement exploités » (62). Ce centre se verra exonéré, par autorisation accordée par arrêté royal délibéré en conseil des ministres, du respect des dispositions relatives aux données « sensibles » — à l'exception des données relatives à la santé régies par l'article 7 de la nouvelle loi — et de celles relatives à l'obligation d'information, aux droits d'accès, de rectification et d'opposition (63). Cette exception ne peut cependant jouer qu'à l'égard des traitements gérés par le Centre « pour la réception, la transmission à l'autorité judiciaire et le suivi des données concernant des personnes qui sont suspectées dans un dossier déterminé de disparition ou d'exploitation sexuelle, d'avoir commis un crime ou un délit ». L'arrêté royal, pris après avis de la Commission de la protection de la vie privée, devra déterminer la durée et les conditions de l'autorisation (64).

1.3. — Le champ d'application territorial

18. — L'article 3*bis* de la nouvelle loi modifie profondément le critère de rattachement permettant de cerner son champ d'application territorial. Cette disposition est essentielle dans un contexte où les traitements sont de plus en plus internationalisés, notamment, par l'utilisation de larges réseaux présents sur différents territoires.

Le critère ne diffère plus selon qu'il s'agit d'un traitement automatisé ou non. La localisation du traitement n'est plus déterminante. Elle est supplantée par le lieu de l'établissement fixe du responsable du traitement.

19. — La loi belge sera en principe applicable dès lors que le traitement « est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public » (65).

Deux éléments méritent d'être précisés.

a. Il faut d'abord que le traitement soit effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement. C'est en effet la loi du territoire sur lequel se situe l'établissement pour lequel le traitement est effectué, qui est applicable (66).

Ainsi, si une entreprise étrangère effectue un traitement sur son territoire, elle ne sera pas soumise à la loi belge si, malgré la présence d'une filiale sur le territoire belge, le traitement n'est pas poursuivi dans le cadre des activités de cette filiale. On peut par exemple penser à des traitements poursuivis dans le cadre d'un site Web ouvert par la maison mère étrangère d'un groupe de sociétés dont une filiale se situe en Belgique, pour autant que les services qui sont prestés via ce site le sont par la seule maison mère, indépendamment de sa filiale belge. Ainsi des commandes de disques peuvent être effectuées sur le Web sans intervention d'une filiale située en Belgique. Le traitement des données poursuivi par la maison mère n'est pas effectué dans le cadre des activités de la filiale belge.

On peut alors se demander quelles sont les implications exactes de l'exigence de la poursuite du traitement dans le cadre des activités de l'établissement. Suffit-il que le traitement profite à ses activités ou qu'il soit poursuivi par l'établissement dans le cadre de ses activités?

Si un groupe de sociétés situées sur le territoire de différents pays européens centralisent sur un même territoire un traitement — par exemple en vue de la gestion des membres du personnel des différentes sociétés —, la loi du lieu de l'établissement de la société qui poursuit effectivement le traitement sera d'évidence applicable. Ce traitement ne risque-t-il pas, en vertu du critère commenté, de se voir appliquer l'ensemble des lois nationales des territoires sur lesquels les sociétés sont situées? Même si ce traitement est situé dans un autre pays, il est poursuivi en partie pour les besoins propres — et donc, dans le cadre des activités — des différentes sociétés du groupe établies sur chacun des autres territoires de l'Union. L'exposé des motifs paraît considérer que dans ce cas, seule la loi du pays où est située la société qui traite les données est applicable à celui-ci. Les autres sociétés, au profit desquelles le traitement est poursuivi, ne seraient soumises qu'à leurs lois dans la mesure où elles effectuent un nouveau traitement à l'aide des données centralisées (67).

Cette solution doit être approuvée. Elle révèle implicitement une autre condition essentielle contenue dans le critère retenu par la loi belge. L'établissement doit participer au traitement des données dans le cadre de ses activi-

tées et quelles finalités exactes d'utilisation sont poursuivies? Pire, comment la Commission pourrait-elle s'immiscer dans les dédales de la sûreté de l'Etat si rien n'est exigé quant à la transparence des traitements?

(58) « La loi consacre un dangereux déséquilibre entre les impératifs légitimes de la sécurité de l'Etat et de sa défense et les intérêts de la personne concernée dans la mesure où la loi affaiblit de manière disproportionnée les possibilités de contrôle du respect des prérogatives liées à la protection des données » (Y. Poullet et B. Havelange, « Secrets d'Etat et vie privée : ou comment concilier l'inconciliable? », *op. cit.*, n° 15).

(59) Toute autorité publique exerçant des missions de police judiciaire bénéficie de l'exception (art. 3, § 5, 1°, de la nouvelle loi). Les services de police visés à l'article 3 de la loi du 18 juillet 1991 se voient reconnaître l'exception en vue de l'exercice de leurs missions de police administrative (art. 3, § 5, 2°, de la nouvelle loi). Il en est de même d'autres autorités publiques désignées par arrêté royal délibéré en conseil des ministres, après avis de la Commission de la protection de la vie privée (art. 3, § 5, 3°, de la nouvelle loi).

(60) Voy. le nouvel article 13, alinéa 1er, de la loi.

(61) La création de ce centre indépendant avait reçu le soutien du gouvernement, annoncé lors de la marche blanche du 20 octobre 1996.

(62) Ci-après dénommé le « Centre ». Il faut rappeler ici que ce Centre est un établissement d'utilité publique constitué par acte du 25 juin 1997. Il a reçu pour mission d'apporter, un support actif à la recherche d'enfants signalés disparus ou enlevés, de prévenir et de lutter, contre la disparition et l'exploitation sexuelle des enfants. Le 30 mars 1998, un protocole de collaboration entre les représentants du Centre, le ministre de la Justice, les cinq procureurs généraux (voy. le texte de celui-ci, *in* annexes du Rapport fait au nom de la Commission de la justice, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 1566/10, p. 203). Lors de l'élaboration de ce protocole, il est apparu que le Centre devrait, à l'occasion de l'exécution de ses missions, enregistrer et traiter, des données à caractère personnel concernant tant les victimes que des tiers suspects ou auteurs d'infractions. L'avis de la Commission de la protection de la vie privée a dès lors été sollicité (Avis n° 10/98 du 12 mars 1998, *in* annexes du Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 1566/10, p. 167). Ce dernier était largement défavorable. Il dénonçait notamment certaines modalités de collecte — par voie téléphonique — et différents traitements envisagés portant sur des données sensibles, médicales et judiciaires. Une base légale a dès lors paru nécessaire pour permettre certaines dérogations aux législations protectrices de la vie privée. Ces différentes exceptions ont alors été prévues dans un projet de loi distinct (voy. projet de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel, *Doc. parl.*, Ch., sess. ord. 1997-1998, n° 1586/1). Elles ont ensuite été insérées dans le projet donnant lieu à la loi commentée.

(63) Voy. les articles 9, 10, § 1er, et 12, de la nouvelle loi.

(64) Le texte légal prévoit différentes garanties permettant de concilier les exceptions aux règles générales de protection avec le respect des droits fondamentaux des personnes concernées par les données, fussent-elles considérées comme suspectes de crimes graves et particulièrement odieux : les traitements dont question ne peuvent en aucun cas déboucher sur la tenue « d'un fichier de personnes suspectes d'avoir commis un crime ou un délit ou de personnes condamnées », la désignation par le conseil d'administration du Centre, parmi les membres du personnel, d'un préposé à la protection des données exerçant ses missions de manière indépendante, la soumission des membres du personnel du Centre et de ceux qui traitent les données au secret professionnel sanctionné par l'article 458 du Code pénal et la soumission de tout enregistrement téléphonique à l'information spécifique de l'appelant pour autant que ce dernier ne s'y oppose pas.

(65) Article 3*bis*, 1°, de la nouvelle loi.

(66) Exposé des motifs, p. 26.

(67) *Idem*.

tés et n'est soumis à la loi que dans la mesure du traitement qu'elle opère sur les données (68). S'il profite donc de données traitées en dehors du territoire, la loi belge ne s'applique qu'aux traitements poursuivis réellement par l'établissement.

b. Il faut ensuite que l'établissement du responsable du traitement pour lequel le traitement est effectué soit situé sur le territoire belge.

La loi, reprenant le principe contenu dans la directive, vise tout établissement fixe du responsable du traitement. L'exposé des motifs se réfère expressément au considérant 19 de la directive selon lequel « l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable ». Ce considérant précise en outre « que la forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard ».

20. — L'article 3*bis*, 2°, de la nouvelle loi détermine un second critère de rattachement dans l'hypothèse où le premier ne trouverait pas à s'appliquer. On vise ici le cas où le responsable du traitement n'a pas d'établissement sur le territoire de la Communauté européenne (69) mais « recourt, à des fins de traitement de données à caractère personnel, à des moyens automatisés ou non, situés sur le territoire belge, autres que ceux qui sont exclusivement utilisés à des fins de transit sur le territoire belge » (70).

Ce critère, issu de l'article 4.1., *c*, de la directive, risque de faire couler beaucoup d'encre et de donner lieu à de nombreuses contestations. La seule explication donnée par la directive est contenue en son considérant 18 qui énonce que : « l'établissement dans un pays tiers, du responsable du traitement de données ne doit pas faire obstacle à la protection des personnes prévue par la présente directive; que, dans ce cas, il convient de soumettre les traitements de données effectués à la loi de l'Etat membre dans lequel des données en cause sont localisées et de prendre des garanties pour que les droits et obligations prévus par la présente directive soient effectivement respectés ». Deux interprétations de l'article 3*bis*, 2°, paraissent pouvoir être défendues.

21. — La première interprétation, extensive, du champ d'application territorial, consiste à appliquer cette disposition à la lettre. Dès lors que le responsable n'a pas d'établissement sur le territoire communautaire mais utilise n'importe quel moyen (71) situé sur le territoire belge en vue de traiter des données à caractère personnel, la loi belge s'appliquerait sous réserve du seul transit des données sur le territoire.

Il en résulterait un phénomène de rattachement de tout traitement situé en dehors de l'Union européenne aux lois nationales dès lors que ce traitement présenterait un lien matériel, si minime soit-il, avec le territoire d'un pays de l'Union, en l'espèce la Belgique. En conséquence par exemple, tout traitement de données à caractère personnel poursuivi dans le cadre d'un site Web dont le serveur est situé dans n'importe quelle partie du monde serait soumis à la loi belge dès lors que ce site permettrait la collecte de ces données par des moyens situés sur le territoire belge — le P.C. du surfeur belge, son logiciel de navigation, les installations de son fournisseur d'accès, les lignes des opérateurs de télécommunication, etc. Cette conséquence est absurde et irréaliste. Elle vide en plus de tout contenu les règles relatives aux flux transfrontières de données vers l'extérieur de la Communauté. Si la loi belge s'applique, il n'est plus besoin de déterminer si le territoire sur lequel les données sont traitées présente un niveau de protection adéquate...

22. — C'est pourquoi on lui préfère une *seconde interprétation* prenant le contre-pied de celle présentée précédemment. La disposition commentée doit se comprendre à la lumière de sa *ratio* et des autres dispositions de la loi, principalement celles relatives aux flux de données vers les pays tiers à la Communauté.

Elle amène à retenir l'application de l'article 3*bis*, 2°, dans deux catégories de situation (72). La première est celle où le responsable du traitement cherche délibérément à contourner les lois nationales prises en vertu de la directive et, pour ce faire, délocalise son établissement dans un pays tiers tout en utilisant encore certains moyens sur le territoire communautaire. La seconde vise le cas où le responsable du traitement réalise, par des moyens propres situés sur le territoire européen, un flux de données vers le pays tiers où il traite les données (73).

Le but de l'article 3*bis*, 2°, est d'éviter que la personne concernée ne soit privée de toute protection suite à l'établissement du responsable en dehors de la Communauté (74). Dans la proposition initiale de la directive, le considérant 10 s'expliquait sur les craintes du législateur européen de voir la personne concernée par les données privée de toute protection en visant explicitement le risque de voir une *délocalisation* du traitement empêcher l'application de la protection. Dès lors que la localisation du traitement n'était plus le critère de rattachement retenu dans la proposition modifiée de directive, ce considérant a été réécrit pour tenir compte du critère du lieu d'établissement du responsable et déboucher sur le texte du considérant 18 de la directive tel que repris ci-avant (75). La *ratio* restait cependant identique. Le but de la disposition est bien d'éviter de voir le responsable du traitement tenter de contourner les législations européennes applicables en s'établissant en dehors de celle-ci alors même que le traitement porte sur des données qui en proviennent et que le bénéfice de ce traitement est à rechercher dans ses activités orientées vers l'Union européenne. On retrouve ici la première catégorie de situations, envisagée ci-avant.

La réglementation particulière sur les transferts de données vers les pays tiers s'applique quant à elle à la plupart des autres hypothèses où les données à caractère personnel relatives à des personnes concernées établies sur le territoire sont traitées par le responsable non établi dans la Communauté. Le traitement de ce dernier nécessitera en effet qu'un transfert ait lieu d'un pays de la Communauté vers le pays tiers où il est établi. Si ce transfert se fait au départ de la Belgique, les articles 21 et 22 de la nouvelle loi s'appliqueront à toute personne à l'origine du flux (76). Le transfert ne pourra avoir lieu — sauf exception — que si le pays destinataire offre un niveau de protection adéquat. La personne concernée n'est donc pas laissée sans protection. Si par contre, seul le responsable intervient au départ d'un pays tiers pour permettre le transfert, sans intermédiaire mais grâce à des moyens techniques situés sur le territoire belge, l'article 3*bis*, 2°, trouverait à s'appliquer. On retrouve ici la seconde catégorie de situation envisagée ci-avant.

(68) Cette solution paraît du reste être en conformité avec l'esprit de la directive. Le considérant 18 de la directive précise en effet que le but est de soumettre tout traitement effectué dans la Communauté à la législation de l'un des Etats membres et qu'il est donc opportun « de soumettre les traitements de données effectués par toute personne opérant sous l'autorité du responsable du traitement établi dans un Etat membre à l'application de la législation de cet Etat » (voy. aussi, l'article 4.1., *a, in fine* de la directive). L'établissement dont on parle ici est donc bien celui qui intervient dans le traitement des données.

(69) A ce propos, l'exemple repris dans l'exposé des motifs n'est pas pertinent. Le Roi raisonne en effet à partir d'une hypothèse où le responsable du traitement est établi sur le territoire belge et traite, dans le cadre des activités de cet établissement, des données à caractère personnel dans un pays en dehors de la Communauté européenne (Exposé des motifs, p. 27). Dès lors que le responsable est établi en Belgique, le critère commenté ne trouve pas à s'appliquer.

(70) Le responsable doit alors désigner un représentant établi sur le territoire belge. Ce dernier assurera le lien nécessaire entre le responsable du traitement situé à l'étranger et les personnes concernées par les données et/ou les autorités de contrôle. Il sera, le cas échéant, responsable du non-respect de la loi sans préjudice d'actions éventuelles intentées contre le responsable lui-même.

(71) D'après l'exposé des motifs, « Le terme "moyens" recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routes, etc. » (p. 27).

(72) Cette interprétation a été défendue en matière d'Internet par M.-H. Boulanger, C. de Terwangne, « Internet et le respect de la vie privée », *op. cit.*, pp. 200 à 204.

(73) On pense notamment au cas où il dépose des cookies sur le disque dur d'un surfeur européen lors de la consultation de son site Web.

(74) Exposé des motifs, p. 27.

(75) Voy. la comparaison des deux textes *in* 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 donnée, Com (92)122 final - Syn 287, *J.O.C.E.*, 27 nov. 1992, n° C311, p. 33.

(76) On peut cependant se demander quelle est la portée exacte du champ d'application territorial des dispositions relatives à la réglementation des transferts de données vers des pays tiers. Ayant un objet propre — le transfert de données du lieu où elles sont situées vers un pays tiers à la Communauté — non défini par la directive, on peut soutenir que les articles 21 et 22 de la loi ont un champ territorial propre : tout transfert de données au départ de la Belgique est visé. Peu importe que la personne à l'origine du transfert soit la personne concernée ou une autre personne distincte d'un établissement du responsable du traitement (seul cas où la loi belge serait applicable en vertu de l'article 3*bis*, 1°, de la nouvelle loi). Tout autre interprétation impliquerait des « trous » dans le champ de protection des transferts de données vers des pays tiers.

2. — LES LIGNES DIRECTRICES DE LA PROTECTION

23. — Les principes de protection prévus par la nouvelle loi sont largement identiques à ceux initialement prévus dans la loi du 8 décembre 1992.

En de nombreux points, la nouvelle loi modifie cependant le système antérieur. Soit qu'il se trouve précisé soit qu'il est complété par certains aspects nouveaux.

On s'attardera d'abord aux principes de finalité des traitements (2.1.) et de qualité des données (2.2.). On analysera ensuite le nouveau régime des données dites « sensibles » (2.3.).

2.1. — Le principe de finalité des traitements

24. — La doctrine relative à l'ancienne loi, relayée par les quelques décisions publiées en la matière, avait longuement insisté sur l'importance du principe de finalité, véritable « pierre angulaire » de la protection (77).

L'article 5 de la loi du 8 décembre 1992 prévoyait deux règles distinctes. La première était contenue dans ce que l'on a dénommé le principe de légitimité. Les finalités devaient être déterminées et légitimes. La seconde était prévue dans le principe de conformité qui postulait que les données devaient être adéquates, pertinentes et non excessive par rapport à la finalité et ne pouvaient être utilisées de manière incompatible avec ces finalités.

On admettait alors qu'à un traitement correspondait toujours une finalité déterminée et légitime permettant le contrôle de la conformité des données traitées par rapport à cette finalité. La nouvelle loi s'écarte quelque peu de cette approche.

Le principe de finalité, tout entier contenu dans l'ancien article 5, fait aujourd'hui l'objet de deux dispositions distinctes. Le principe de légitimité des traitements est partiellement réglementé par l'article 4 et fait l'objet de l'article 5 de la nouvelle loi. Le principe de conformité est repris à l'article 4 de la loi qui, en outre, comporte également une obligation d'exactitude des données ainsi que le droit à l'oubli reconnu à la personne concernée.

2.1.1. — *Le principe de légitimité des traitements*

25. — Sous l'ancienne loi, le responsable du traitement définissait *a priori* la finalité d'utilisation des données en étant seulement bridé par une règle de proportionnalité. La finalité ne pouvait impliquer d'elle-même une atteinte disproportionnée aux droits et libertés individuels de la personne concernée au nom des intérêts poursuivis par le responsable du traitement.

L'article 4, 2°, reprend à son compte un énoncé analogue du principe tel qu'il apparaissait dans l'ancienne loi : « Les données à caractère personnel doivent être (...) 2° collectées pour des finalités déterminées, explicites et légitimes (...) ». On renvoie donc ici aux commentaires consacrés à cette disposition (78).

L'article 5 actuel précise que les traitements ne peuvent être opérés que dans l'un des cas visés par cette disposition. Cette dernière transpose très exactement l'article 7 de la directive (79). Il en résulte que tout traitement doit, impérativement, pouvoir se fonder sur une des situations décrites sous peine d'être contraire à la disposition (80).

26. — Le traitement peut d'abord avoir lieu « si la personne concernée a indubitablement donné son consentement ». Le consentement dont il s'agit doit bien évidemment répondre aux conditions contenues dans la définition donnée en préliminaire par la loi (81).

Le traitement se justifie également *a priori* s'il est « nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ». Les traitements nécessaires à l'exécution d'un service demandé ou de la livraison d'un bien acheté par la personne concernée en sont des exemples d'application.

La disposition permet aussi le traitement de données « nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ». On peut citer à titre d'exemple des obligations qui s'imposent aux employeurs, tels la tenue d'une comptabilité particulière ou un registre du personnel accessible aux inspecteurs chargés du contrôle de la législation sociale, la communication de certaines données de leur personnel aux organismes de sécurité sociale, etc.

Le traitement des données est également permis s'il est « nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ». Le considérant 31 de la directive, rappelé dans l'exposé des motifs (82), précise qu'on vise la protection d'« un intérêt essentiel à la vie de la personne concernée ». Cette disposition pourrait fonder le traitement de données dans les cas où la personne concernée se trouve dans une situation d'urgence médicale.

Le traitement peut être aussi fondé s'« il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ». On vise ici les traitements poursuivis dans le secteur public au sens large. Si l'on effectue le rapprochement avec la règle de légitimité, on retrouve les principes administratifs de légalité, spécialité et proportionnalité (83).

Enfin, l'article 5 admet la mise sur pied d'un traitement s'« il est nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée ». Cette disposition diffère quelque peu des hypothèses précédentes. Alors que ces dernières précisaient des situations où l'équilibre des intérêts en présence est *a priori* respecté, la présente disposition rappelle de manière plus explicite le contenu même de la règle de proportionnalité inhérente au principe de légitimité. Même si le traitement est nécessaire au responsable, il ne pourra être poursuivi dès lors que l'opposition des intérêts en présence se résout en faveur de la personne concernée.

Le Roi peut, par arrêté délibéré en conseil des ministres et après avis de la Commission de la protection de la vie privée, préciser les cas où cette dernière situation est considérée comme n'étant pas remplie.

27. — L'articulation entre les articles 4, 2° et 5, de la nouvelle loi doit être bien comprise.

Le respect de l'article 5 n'emporte pas de lui-même le respect de l'article 4, 2°, ou de toute autre règle contenue dans la loi. Le fait de remplir une des conditions de l'article 5 n'implique pas que l'exigence de légitimité de l'article 4, 2°, soit *ipso facto* rencontrée. Les différentes dispositions doivent au contraire s'appliquer cumulativement (84). Ainsi, le consentement de la personne concernée ne permet pas nécessairement — même si ce sera souvent le cas — de légitimer la finalité du traitement (85).

---

(77) Voy. principalement, Th. Léonard, 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, pp. 231 et s.; S. Gutwirth, « De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.*, 1993, p. 1409 et s.; sur l'application de ce principe en jurisprudence, voy. par ex., Com. Anvers, prés., 7 juill. 1994 et Comm. Bruxelles, prés., 15 sept. 1994, *Computerr.*, 1994, pp. 244 et s. et note J. Dumortier et Fr. Robben; *D.I.T.*, 1995, p. 55 et note O. Lesuisse; pour d'autres commentaires sous ces décisions, voy. *D.C.C.R.*, 1994, pp. 83 et s. et note Th. Léonard; S. Gutwirth, « De ontdekking van de *privacy* van de burgers als doeltreffend wapen in de strijd tussen concurrenten », note sous Comm. Bruxelles, réf., 15 sept. 1994, *Jaarboek Handelspraktijk - 1994*, Diegem, Kluwer Rechtswetenschappen, 1995, pp. 361 et s.; J.-P. Buyle, L. Lannoye, Y. Poullet et V. Willems, « Le droit de l'informatique - Chronique de jurisprudence (1987-1994) », *J.T.*, 1996, p. 236, n° 72.

(78) *Idem*. L'exigence d'une finalité « explicite », non exprimée dans l'ancienne version de la disposition, ne modifie pas la portée de la disposition. Elle implique que toute finalité implicite est à bannir, ce qui découlait déjà du principe de transparence issu de l'exigence de détermination de la finalité.

(79) Voy. La protection des données à caractère personnel en droit communautaire, pp. 147 et 148.

(80) Le contrôle du respect du principe de finalité n'est pas modifié par le fait que désormais, à un seul traitement peut correspondre différentes finalités. Ce contrôle s'effectuera toujours à l'égard de chacune des finalités du traitement. Ainsi, le consentement informé impliquera que la personne concernée devra, en connaissance de cause, consentir aux diverses finalités de traitement des données la concernant.

(81) Voy. *supra*, n° 7.

(82) Exposé des motifs, p. 32.

(83) Cf. Th. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », *op. cit.*, p. 242, n^{os} 15 et 260, n° 43; il faut par ailleurs ne pas perdre de vue les exigences de l'article 8, § 2, C.E.D.H.

(84) Voy. Exposé des motifs, p. 31; voy. aussi les considérants 28 et 30 de la directive.

(85) Le fait que l'article 6, § 1er, *b*, de la directive parle de finalités légitimes et que l'article 7 soit intitulé « Principes relatifs à la légitimation des traitements de données » pourrait laisser croire le contraire (voy. égalem. la version anglaise). Le texte

Si l'on veut pousser plus avant la comparaison entre les deux dispositions, on pourrait dire que l'article 5 prévoit des situations abstraites dans lesquelles l'équilibre des intérêts en présence est normalement respecté sans préjudice d'un contrôle concret permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu (86).

28. — Au principe décrit ci-avant s'ajoute une règle issue de la Convention n°108 du Conseil de l'Europe. L'article 4, § 1er, 1°, dispose que les données doivent être traitées loyalement et licitement.

Pour être *licite* un traitement de données doit respecter l'ensemble des prescrits légaux et réglementaires applicables. La *loyauté* du traitement évoque, quant à elle, la transparence des opérations propres au traitement. Cette transparence doit être assurée dès la collecte, notamment par le biais de l'obligation d'informer la personne concernée. Cette dernière doit savoir quel est le but d'utilisation des données, entre quelles mains elles se trouvent, à quelles fins elles sont communiquées, etc. (87). Lorsque des données sont destinées à être traitées hors du territoire communautaire, le traitement ne devrait être considéré comme loyal que si l'on informe les personnes concernées de ce fait.

2.1.2. — *Les principes de conformité et de qualité des données*

29. — L'article 4, 3°, reprend *mutatis mutandis* le contenu du principe de conformité des données déjà présent dans l'ancienne loi. Les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

L'article 4, § 1er, 2°, apporte également une autre précision inhérente au principe de conformité. Les données ne peuvent être traitées ultérieurement de manière incompatible avec les finalités annoncées. La loi précise cependant que la compatibilité doit tenir compte de tous les facteurs pertinents, « notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».

Le recours aux prévisions raisonnables de l'intéressé pour appréhender la compatibilité des données doit être accepté (88). Il comprend en lui-même l'exigence de transparence des traitements qui interdit que la personne ne soit laissée dans la méconnaissance de l'utilisation des données la concernant. Le recours aux dispositions légales et réglementaires est par contre critiquable. On ne peut en effet admettre qu'une nouvelle finalité soit considérée automatiquement « compatible » avec la finalité initiale par le simple fait que ce changement trouve sa source dans une modification légale ou réglementaire (89).

30. — L'attention avait déjà été attirée sur une ambiguïté issue de l'article 6, *b*, de la directive, inséré en droit belge par l'article 4, § 1er, 2° (90). Cette disposition empêchait-elle le responsable du traitement de modifier la finalité d'un traitement déjà en cours, en dehors de la marge laissée par la règle de compatibilité? La réponse faite à l'époque avait cependant été rendue malaisée du fait de l'absence de toute interprétation claire du législateur européen sur la portée de la disposition (91).

L'exposé des motifs de la nouvelle loi est à peine plus explicite. D'après le ministre, la règle « signifie que des données collectées en vue d'une finalité spécifique et explicite et légitime ne pourront être traitées pour une autre finalité incompatible avec la finalité initiale sans que la personne y ait donné son consentement » (92). On ne peut qu'être étonné par cette déclaration. Elle fait du consentement de la personne concernée une condition nécessaire à tout changement de finalité qui est, *a priori*, incompatible avec la finalité initialement annoncée. On ne perçoit pas le fondement de l'opinion exprimée par le ministre. Le consentement n'est pas, on l'a vu, la seule possibilité de légitimer une finalité d'utilisation des données à caractère personnel. Pourquoi dès lors n'admettre ce changement qu'en cas de consentement donné par la personne concernée?

Ce raisonnement, tout erroné qu'il soit, confirme cependant la possibilité laissée au responsable du traitement de modifier fondamentalement une finalité d'utilisation des données (93). Cette modification impliquera cependant la naissance d'un nouveau traitement au sens de la loi. Le responsable devra alors respecter l'intégralité des dispositions de la loi concernant celui-ci. Ainsi par exemple, ce nouveau traitement ne pourra être admis que s'il se fonde sur une des situations visées par l'article 5 de la nouvelle loi, et devra donner lieu, le cas échéant, à une nouvelle déclaration auprès de la Commission, à une nouvelle information de la personne concernée, etc. (94).

31. — L'article 4, § 1er, 4°, de la loi rappelle que les données traitées doivent être exactes et, si nécessaire mises à jour. Il précise en outre que « toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement soient effacées ou rectifiées ».

Il s'agit donc clairement d'une obligation de diligence qui est mise à charge du responsable du traitement (95). Le critère à prendre en compte sera donc celui du responsable normalement prudent et diligent. Il est toutefois intéressant de souligner que la loi invite, pour l'évaluation de la portée de l'obligation, à prendre en compte la finalité poursuivie par le traitement. Cette précision, présente dans la directive, pourrait étonner *a priori*. Elle se justifie néanmoins car, en la matière, la finalité poursuivie est une circonstance de fait essentielle à prendre en compte dans l'évaluation du comportement du responsable du traitement (96).

32. — L'article 4, 5°, précise enfin que les données sont « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement ». On retrouve ici l'idée du droit à l'oubli de la personne concernée. L'adéquation, la pertinence et le caractère non excessif de l'information dépendent du facteur temps. Si la finalité du traitement n'exige plus l'utilisa-

néerlandais de la directive lève l'ambiguïté. En son article 6, il dispose que « De Lid Staten bepalen dat de persoonsgegevens voor een welbepaalde uitdrukkelijk omschreven en *gerechtvaardigde* doeleinde moeten worden verkregen... » alors que l'article 7 est intitulé « Beginselen betreffende de *toelaatbaarheid* van gegevensverwerking ». Autrement dit, l'article 7 n'indique que des principes d'admissibilité du traitement sans préjudice des autres dispositions de la directive. Ce raisonnement est explicitement repris dans Exposé des motifs (p. 31).

(86) Voy. la déclaration de la secrétaire de la Commission de la protection de la vie privée qui parle à ce propos d'une présomption d'équilibre des intérêts dans le cas où une situation prévue par l'article 5 est rencontrée (Rapport, p. 47).

(87) Voy. l'article 9 de la loi qui, réglant le droit d'information de la personne concernée, se réfère explicitement à la loyauté pour déterminer si oui ou non des informations supplémentaires doivent être fournies à la personne concernée par les données.

(88) La disposition entérine la proposition faite, *in* La protection des données à caractère personnel en droit communautaire, p. 146, n° 32.

(89) C'est d'autant plus vrai que les autorités publiques qui modifieraient une finalité d'utilisation suite à un changement de loi ne devraient normalement pas en informer la personne concernée par les données (cf. *infra*, n° 46). L'exposé des motifs paraît d'ailleurs rejeter, une compatibilité automatique lorsqu'il énonce que « la mesure dans laquelle et la manière dont les personnes concernées ont préalablement été informées du nouveau traitement par les autorités jouera un rôle important lors de l'évaluation de la compatibilité ou de l'incompatibilité du traitement avec la finalité initiale pour laquelle les données ont été obtenues » (p. 30).

(90) Voy. La protection des données à caractère personnel en droit communautaire, pp. 146 et 147, nos 30 à 34.

(91) Voy. cependant le considérant 39 de la directive qui admet la légitimité d'une communication des données à un tiers même si cette communication n'était pas initialement prévue.

(92) Exposé des motifs, p. 29.

(93) Le Roi l'admet du reste explicitement en ce qui concerne les autorités publiques (*idem*).

(94) La loi prévoit explicitement un assouplissement pour les traitements à finalités historiques, statistiques ou scientifiques qui ne pourront être réputées incompatibles dès lors qu'ils sont effectués conformément aux règles à définir par arrêté royal.

(95) L'article 16, § 2, de la nouvelle loi — identique à l'article 16, § 1er, 3°, de l'ancienne loi — oblige le responsable « à faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8 ».

(96) On peut penser par exemple à une banque de données rédactionnelles tenue par un organe de presse ou à des banques de données utilisées aux fins de recherches scientifiques. En amont du travail de publication des informations ou de présentation des résultats d'une recherche, les journalistes et les chercheurs ont besoin de traiter librement de l'information qui pourra s'avérer, dans un stade ultérieur de leur travail, inexacte, erronée ou incomplète. La portée de l'obligation d'exactitude doit s'apprécier en fonction de la finalité poursuivie. Dans l'exemple, deux finalités apparaissent. Les données sont d'abord collectées et traitées à l'état brut en vue de permettre un accès aisé à leurs utilisateurs qui, précisément, désirent traiter l'information en vue de la « faire parler » notamment, au moyen de recoupements, de classements, etc. C'est la première finalité d'utilisation des données. L'obligation d'exactitude est, à ce stade, relativement peu contraignante. Les données sont ensuite traitées en vue de leur publication ou de la présentation des résultats. C'est la seconde finalité d'utilisation des données. L'obligation d'exactitude doit être, à ce stade, appréciée plus strictement.

tion des données, leur effacement s'impose (97).

33. — On doit enfin noter que l'admission de différentes finalités pour un même traitement ne remet pas en cause l'application des principes énoncés ci-avant au regard de chaque finalité du traitement. L'adéquation, la pertinence, le caractère non excessif ou exact d'une donnée ne peut se contrôler qu'au regard d'une finalité spécifique. Il en est de même pour l'évaluation de la durée de conservation. C'est pourquoi il est essentiel que la personne concernée par les données puisse distinguer clairement à quelles données se rapporte chacune des finalités (98).

2.2. — Le traitement des données « sensibles »

34. — L'ancienne loi distinguait trois types de données sensibles pour lesquelles l'interdiction de traitement était la règle sauf exceptions prévues par la loi. Il s'agissait des données « sensibles » au sens strict, des données judiciaires et des données médicales.

La nouvelle loi ne modifie ni cette distinction, ni le principe d'interdiction qui gouverne le traitement de ces données. Par contre, elle modifie largement le régime des exceptions.

2.2.1. — *Les données « sensibles » au sens strict*

35. — L'article 6 énonce les données à caractère personnel communément qualifiées de sensibles. Il s'agit des données « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que (les) données relatives à la vie sexuelle ».

La liste ne diffère de celle prévue précédemment que par la disparition des données « mutualistes ». Cette dernière catégorie n'apparaissait pas dans la liste limitative prévue par la directive (99).

36. — La notion même du caractère sensible ou non de la donnée paraît modifiée. Sous l'ancienne loi, des divergences d'interprétation étaient apparues (100). En effet, une interprétation stricte du principe d'interdiction avait comme conséquence de proscrire des traitements assurément légitimes comme le fait qu'un passager d'un avion mangeait « kasher » ou qu'un virement comportait la mention du paiement d'une cotisation à un parti politique.

La Commission de la protection de la vie privée avait proposé de distinguer les données directement sensibles, seules soumises à la règle de l'interdiction de traitement, des données indirectement sensibles (101). Elle n'avait pas été suivie par le ministre qui, quant à lui, distinguait selon qu'il était possible ou non de déduire directement l'information sensible des données enregistrées (102). Ainsi, les données d'un fichier de membres d'un parti seraient des données sensibles au contraire de données d'un fichier relatif à la clientèle, révélant l'achat de bibles ou du Coran. Une distinction fondée sur l'existence ou non d'un traitement portant sur l'information sensible avait été proposée (103). Le débat ne s'était cependant pas amplifié du fait du grand nombre d'exceptions prévues par arrêté royal.

A l'époque, le texte de l'article 6 visait des données seulement « relatives » aux informations sensibles telles que l'origine raciale ou ethnique. Désormais, la nouvelle disposition vise plus largement, les données « révélant » une telle information, sauf en ce qui concerne la vie sexuelle (104). Le ministre réaffirme donc son interprétation en se fondant sur ce changement — malheureux — de terminologie : « Cette formulation est donc plus large que celle de l'actuel article 6 dans la mesure où les données ne doivent pas nécessairement se rapporter directement aux origines raciales ou ethniques, etc. mais qu'il suffit que la race ou l'origine ethnique puissent être déduites des données » (105).

On se rend aisément compte à quel point cette interprétation est absurde. Ainsi, si un fichier relatif à des mauvais payeurs comporte des données relatives à M. Ben Ali ou Mme Mokambe, ces informations deviennent *a priori* interdites de traitement puisqu'elles « révèlent » assurément, par le nom des personnes concernées, une origine raciale ou ethnique. Il en est de même des traitements permettant l'exécution d'un virement au bénéfice d'un syndicat, portant la mention « cotisation 1999 » qui « révèle » sans doute possible l'appartenance syndicale. Le ministre paraît quelque peu s'en rendre compte puisqu'il ajoute que « cette disposition doit naturellement être appréciée de manière raisonnable au sens où les informations sensibles doivent pouvoir être déduites des données avec certitude ou avec une probabilité quasi certaine. On ne peut conclure par exemple à la conviction religieuse d'une personne avec certitude ou avec quasi-certitude sur la base du seul fait qu'elle commande un exemplaire de la Bible à une société de vente par correspondance ».

Doit-on préciser que l'explication donnée ne convaincra personne. Les exemples cités ci-avant ne reçoivent aucune solution. Le texte ne comporte en outre aucune distinction selon l'intensité de la « révélation » induite des données. Sa violation est du reste sanctionnée pénalement ce qui exclut *a priori* un critère aussi flou que celui proposé par le ministre. Enfin, même si l'information sensible n'est pas certaine « objectivement », elle peut l'être « subjectivement » pour celui qui traite les données et fonder, le cas échéant, de véritables discriminations basées sur l'exploitation de cette « fausse » information (106).

37. — Dès lors que le traitement porte sur des données qui révèlent une des informations dont question ci-avant, il est *a priori* interdit. Le responsable du traitement devra alors pouvoir se fonder sur une des treize exceptions prévue par le paragraphe 2 du nouvel article 6. Cette liste est désormais limitative puisque le Roi n'est plus habilité à prévoir les cas d'exemptions.

La plupart de ces exceptions sont connues et avaient déjà été insérées en droit belge par arrêté royal. Ainsi, l'interdiction est levée si la

(97) Le Roi peut prévoir, après avis de la Commission de la protection de la vie privée, des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de cette période, à des fins historiques, statistiques ou scientifiques.

(98) On peut se demander si un critère simple de compatibilité n'apparaît pas de la constatation précédente. Les auteurs de la directive, tout comme le législateur belge, ne peuvent définir de manière exacte ce qu'est la finalité d'un traitement. Notion éminemment fluctuante, elle ne se conçoit que de manière concrète par les différents usages des données entrepris par le responsable du traitement. Il est particulièrement malaisé de déterminer les différents ensembles d'opérations portant sur les données qui génèrent des finalités d'utilisation différentes. Il est donc plus facile d'admettre qu'un seul traitement puisse déboucher sur une ou plusieurs finalités d'utilisations définies de manière plus ou moins larges selon les cas. Les principes de conformité et de qualité des données permettent cependant de « récupérer » une cohérence qui paraît aujourd'hui un peu hypothétique. Le traitement poursuit des finalités compatibles entre elles dès lors que l'application des principes énoncés ci-avant n'est pas fondamentalement modifiée. Ainsi, la finalité gestion de compte peut se définir de manière générique ou de manière spécifique en visant diverses utilisations induites de la première : mise à jour de l'avoir en compte, gestion du porte-monnaie électronique lié à une carte, gestion des différentes cartes liées au compte, etc.

(99) Exposé des motifs, p. 33.

(100) Sur ce débat, voy. Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *op. cit.*, pp. 29 à 31, n° 380.

(101) Avis n° 7/93 du 6 août 1993 de la Commission de la protection de la vie privée relatif au traitement de données sensibles, au sens de l'article 6 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.*, 28 février 1995, p. 4420, n° 8.

(102) Rapport au Roi précédant l'arrêté royal n° 14 du 22 mai 1996 déterminant les fins, les critères et les conditions des traitements autorisés de données visées à l'article 6 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.*, 30 mai 1996, p. 14515.

(103) Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *op. cit.*, p. 30.

(104) En conformité avec le texte de l'article 8.1. de la directive.

(105) Exposé des motifs, pp. 33 et 34.

(106) Le débat sur les données sensibles est mal posé. Le caractère sensible d'une information se révèle bien plus par l'utilisation que l'on en fait que par sa nature intrinsèque. Une rédaction d'un journal d'extrême gauche traite les données de sa clientèle en vue de gérer les abonnements de ses lecteurs. Les données révèlent une information quant aux opinions politiques des lecteurs. Pourtant, le caractère « sensible » n'est pas exploité par le responsable du traitement. Une interdiction de traitement *a priori* ne se justifie donc pas : l'information sensible n'est pas traitée puisqu'elle n'est transcendée par aucune finalité d'utilisation. Le même journal vend son fichier à un groupuscule d'extrême gauche désireux de toucher un électorat potentiel. Ce fichier est ensuite saisi par la sûreté de l'Etat en vue d'un contrôle accru des sympathisants du groupe, considéré comme « terroriste » par la sûreté de l'Etat. La finalité des traitements porte alors précisément sur le caractère sensible de l'information. C'est l'appartenance politique présumée qui justifie l'achat du fichier et sa saisie par la sûreté de l'Etat. La communication du fichier des abonnés devrait donc être interdite *a priori* sauf à bénéficier d'une exception légale. C'est donc bien plus le traitement envisagé qui tend ou non à « révéler » une information sensible que la nature de la donnée elle-même. Une telle interprétation pourrait peut être se justifier par un appel à la version néerlandaise de la disposition commentée plus ambiguë sur ce point (voy. aussi la version néerlandaise de l'article 8 de la directive).

personne concernée a donné son consentement par écrit au traitement, si le traitement est nécessaire à l'exécution des obligations du responsable du traitement et à l'exercice de ses droits en matière de droit du travail ou est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, si le traitement porte sur des données manifestement rendues publiques par la personne concernée, si le traitement est nécessaire à la recherche scientifique dans les conditions déterminées par le Roi ou sous certaines conditions, si le traitement est nécessaire à des fins médicales (médecine préventive, diagnostic médical, administration de soins de santé ou de traitements à la personne concernée ou à un parent) et à des fins de gestion des services de santé pour autant que le traitement soit effectué sous la surveillance d'un professionnel des soins de santé (107).

D'autres exceptions paraissent plus contestables en ce qu'elles frappent par l'étendue de leur champ d'application :

— Toute fondation, association ou autre organisme non lucratif à finalité politique, philosophique, religieuse, mutualiste ou syndicale jouit de la levée de l'interdiction dès lors que le traitement est effectué dans le cadre de ses activités légitimes et se rapporte aux seuls membres de cet organisme ou « aux personnes entretenant avec lui des contacts réguliers liés à sa finalité ». On ne peut être que frappé par le flou de cette dernière expression. Comme l'exige la directive, les données ne peuvent dans ce cas être communiquées à des tiers sans le consentement des personnes concernées (108). Cette disposition élargit indûment la portée de l'exception prévue par la directive. En effet, celle-ci prévoit explicitement que l'exception est conditionnée par la prise « de garanties appropriées » en faveur des personnes concernées. Ces garanties devaient être précisées par le législateur. La plus évidente d'entre elles implique une définition claire par le législateur des finalités d'utilisation des données sensibles. L'exception commentée ne vise en effet qu'à déterminer les bénéficiaires de l'exception.

— Tout traitement considéré comme nécessaire à la réalisation d'une finalité fixée par ou en vertu d'une loi, en vue de l'application de la sécurité sociale tombe hors du champ d'application de l'interdiction. Comme on le verra ci-après, les organismes de sécurité sociale jouissent en Belgique d'une situation privilégiée. Ils bénéficient de toutes les exceptions possibles au régime de protection légale. Le traitement des données sensibles n'y échappe pas. Le critère de nécessité du traitement par rapport aux finalités légales ou réglementaires ne convainc pas. Le traitement peut être techniquement nécessaire à la réalisation d'une finalité légale — par exemple une gestion plus rationnelle du système — tout en impliquant une ingérence disproportionnée dans les droits et libertés individuelles. Ce risque aurait à tout le moins justifié la prise de garanties spécifiques légitimant la levée de l'interdiction. Ces garanties sont du reste imposées par la directive elle-même pour toute dérogation au nom d'un intérêt public important auquel se réfère le Roi pour fonder la présente exception (109). On ne trouve nulle trace de telles garanties dans la loi.

— Tout traitement de données sensibles permis par une loi, un décret ou une ordonnance pour un autre motif important d'intérêt public (110) est exempte de l'interdiction de traiter les données sensibles. Outre qu'ici aussi, aucune garantie spécifique n'est exigée par la loi, on peut s'interroger également sur la portée à reconnaître au motif d'intérêt public important. Ce concept devrait être éclairé par le paragraphe 2 de l'article 8 de la convention européenne des droits de l'homme qui indique les seuls buts admissibles pour justifier une ingérence par l'autorité publique dans la vie privée des citoyens.

Le Roi détermine par arrêté délibéré en conseil des ministres, après avis de la Commission de la protection de la vie privée, les conditions particulières auxquelles doit satisfaire le traitement des données sensibles bénéficiant d'une dérogation à l'interdiction. Il reste à espérer que ces dispositions prévoient bien toutes les garanties appropriées à chaque exception rendant celle-ci plus acceptable.

2.2.2. — *Les données relatives à la santé*

38. — Le régime des données « médicales » a fait l'objet d'un profond remaniement (110*bis*).

Outre un changement de terminologie — on parle désormais de « données relatives à la santé » — le nouvel article 7 de la loi ne définit plus ce qu'il faut entendre par ce type de données. Précédemment, on entendait 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 et aux soins médicaux ».

L'exposé des motifs invite à reconnaître une portée plus étroite à la donnée « relative à la santé » (111). Alors que les données qui « révèlent » une information sensible visent toute information sensible « déduite » de la donnée — comme visé précédemment dans la définition de la donnée médicale — celles qui sont seulement « relatives » à la santé doivent « se rapporter » à ces informations. Le ministre en conclut que « Des données qui révèlent seulement l'état de santé ou la vie sexuelle d'un individu, mais qui ne se rapportent pas à sa santé ou à sa vie sexuelle, ne tombent pas sous le régime — plus strict — de l'article 8 de la directive ». On peut penser ici à une photographie « révélant » un handicap.

On a déjà souligné le manque de clarté de cette distinction. Appliquée aux données relatives à la santé, on peut par exemple se demander ce qu'il en est désormais des traitements administratifs et comptables concernant des soins et traitements médicaux. Antérieurement explicitement exclus de la définition, on pourrait tenter de leur appliquer la distinction contenue dans l'exposé des motifs. Ces dernières ne se rapporteraient pas directement à l'information relative à la santé et ne seraient donc pas visées par l'actuel article 7. On peut s'attendre cependant à de lourdes hésitations en pratique (112).

39. — L'article 7 interdit le traitement de données relatives à la santé tout en prévoyant un très grand nombre d'exceptions à ce principe.

La plupart de ces exceptions sont identiques à celles prévues pour les données « sensibles » au sens strict. On vise ici le consentement écrit de la personne concernée, le traitement nécessaire à l'exécution d'obligations issues du droit du travail, le traitement nécessaire à l'application de la sécurité sociale, le traitement rendu obligatoire par la loi, le décret ou l'ordonnance pour des motifs importants d'intérêt public, celui nécessaire à la défense d'intérêts vitaux de la personne concernée ou d'une autre personne si la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, le traitement portant sur des données manifestement rendues publiques par la personne concernée, le traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice et le traitement nécessaire à la recherche scientifique.

(107) Sur cette expression, voy. *infra*, n° 40.

(108) On peut se demander s'il est bien normal que le monde politique se mette à l'abri de toute difficulté à l'égard de règles protectrices imposées à ses administrés.

(109) Exposé des motifs, p. 35. Le ministre se justifie par un appel à « un motif d'intérêt public important », notion qu'il éclaire par le considérant 34 de la directive qui énonce que « les Etats membres doivent également être autorisés à déroger à l'interdiction de traiter, des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale — particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie (...) ». Il étend cependant indûment la portée du considérant. Ce dernier n'identifie pas automatiquement les domaines de la santé publique et de la protection sociale comme porteurs d'un motif important d'intérêt public permettant une dérogation générale à l'interdiction de traitement des données sensibles. Il ne vise du reste pas une dérogation générale à l'interdiction de traitement de toutes les données sensibles visées par la disposition mais de certaines catégories de données sensibles. Ce considérant invite plutôt à réfléchir sur l'existence de motifs d'intérêt public importants dans certains domaines — par exemple le domaine de la sécurité sociale — qui permettrait certaines dérogations spécifiques, par exemple en cas de collecte de données sensibles lors de demandes de prestations et de services dans le régime d'assurance maladie. La disposition commentée ne s'embarrasse quant à elle d'aucune nuance : l'application de la sécurité sociale y est considérée comme étant en elle-même le motif d'intérêt public important. On peut en outre se demander pourquoi l'application de la sécurité sociale se voit ainsi privilégiée par rapport à l'application du régime fiscal, du régime linguistique, de la matière de l'enseignement, etc.

(110) On sera attentif à la différence de terminologie entre l'exception prévue pour les données commentées et celle, analogue, prévue pour les données relatives à la santé. Dans ce dernier cas, le traitement doit être rendu « obligatoire » par la loi, le décret ou l'ordonnance et non seulement « permis » par ceux-ci.

(110*bis*) Il est à noter que la directive parle de données « révélant » l'état de santé et non de données « relatives » à l'état de santé.

(111) Exposé des motifs, p. 34; voy. cependant à la page 38, la déclaration selon laquelle les données relatives à la santé seraient une catégorie de données plus large que les données médicales...

(112) Le remplacement des « praticiens de l'art de guérir » aux « professionnels des soins de santé » plaiderait par contre pour l'inclusion des données administratives dans la catégorie des données relatives à la santé.

On retrouve également le traitement nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de soins de santé agissant dans l'intérêt de la personne concernée. Les données doivent alors être traitées sous la surveillance d'un professionnel des soins de santé.

En outre, ne sont pas soumis à l'interdiction de traitement ceux nécessaires à la promotion et à la protection de la santé publique, y compris le dépistage et ceux nécessaires pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée.

40. — Toutes ces exceptions ne sont admises que si les traitements des données relatives à la santé sont effectués sous la responsabilité d'un professionnel des soins de santé, sauf en cas de consentement de la personne concernée ou de nécessité pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée.

On peut se demander ce qu'il faut entendre par la notion de « professionnel des soins de santé » (113). Suite à une remarque analogue de la Commission de la protection de la vie privée (114), l'exposé des motifs s'est attaché à éclaircir la notion, sans toutefois y parvenir (115).

Antérieurement, l'article 7 visait les seuls « praticiens de l'art de guérir » à savoir les médecins, dentistes, pharmaciens et accoucheuses, sous la responsabilité desquelles, sauf consentement de la personne concernée, les données médicales devaient être traitées. L'exposé des motifs relève qu'en pratique, le principe était difficile à appliquer, la catégorie des praticiens de l'art de guérir étant trop limitée (116).

C'est pourquoi il a été décidé d'étendre la possibilité de traitement aux professionnels des soins de la santé tenus à une obligation de secret. Ces termes correspondraient « à un concept vaste qui fait référence à l'ensemble des personnes qui prestent des soins de santé à l'égard d'autres personnes dans l'exercice de leur profession » (117). Mais l'exposé vise également les personnes travaillant pour le compte de professionnels des soins de la santé. Une justification est proposée par référence au texte de l'article 8.3. de la directive qui vise tant le professionnel des soins de la santé soumis par le droit national au secret professionnel qu'à d'autres personnes soumises à une obligation de secret équivalente. Toute énumération est cependant rejetée et l'alinéa 2 du paragraphe 4 de la nouvelle disposition prévoit que le Roi pourra déterminer ce que recouvre la notion en cause.

Il restait une difficulté à résoudre. Une garantie élémentaire pour la protection des données relatives à la santé est la soumission des personnes qui traitent de telles données à une obligation de secret. La Commission avait proposé de limiter la catégorie de « praticien de la santé » aux personnes tenues à une obligation de secret par ou en vertu d'une disposition légale, sanctionnée pénalement (118). L'exposé des motifs explique que l'exigence est rencontrée par la nouvelle disposition (119). Au lieu de se référer à une obligation de secret préexistante, l'alinéa 3 du paragraphe 4, prévoit que « le professionnel des soins de santé et ses préposés ou mandataires sont soumis au secret ». L'article 39, 3°, érigeant la violation de l'article 7 par le responsable du traitement, ses préposés ou mandataires, l'exposé des motifs y voit donc une obligation de secret sanctionnée pénalement. Les personnes intervenant dans le traitement des données relatives à la santé sont donc tenues à une sanction pénale distincte de l'article 458 du Code pénal (120).

Le raisonnement à la base du nouvel article 7 est illogique et ne permet pas de déterminer avec précision qui sont ces « professionnels des soins de santé » qui endossent la responsabilité du traitement des données relatives à la santé. La notion devient impossible à préciser puisque le texte se refuse à la définir. D'autre part la référence à l'obligation de secret devient inopérante, ces professionnels, comme leurs préposés ou mandataires, étant toujours soumis à l'obligation de secret créée par la loi elle-même.

41. — On doit encore relever que le Roi est chargé de déterminer les conditions particulières des traitements bénéficiant de l'exception au principe d'interdiction.

En outre, en vertu du paragraphe 5 de l'article 7, les données relatives à la santé ne peuvent normalement être collectées qu'auprès de la personne concernée. Le but est ici de permettre à la personne concernée de contrôler les communications des données relatives à sa santé. Ces dernières ne peuvent être collectées auprès d'autres sources que si elles respectent les conditions visées par la disposition : la collecte doit être conforme aux conditions prescrites par le Roi, être effectuée sous la responsabilité du professionnel des soins de santé et être nécessaire à la finalité poursuivie. Ces conditions paraissent pouvoir ne pas être respectées dès lors que la personne concernée n'est pas en mesure de fournir les données elle-même. On peut toutefois se demander si le principe ne sera pas vidé de sens par ses exceptions. Si le responsable du traitement a besoin de se procurer des données médicales sur son patient auprès d'autres sources, n'est-ce pas précisément parce que la personne concernée est incapable matériellement de lui transmettre les informations demandées?

2.2.3. — *Les données « judiciaires »*

42. — La modification de l'article 8 est également fondamentale.

Les données communément reprises sous le qualificatif de « judiciaires » reçoivent une définition particulièrement large. Il s'agit « des données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté ». Leur traitement est également *a priori* interdit.

Cette définition élargit celle présente dans la directive. Cette dernière ne visait ni les données relatives aux suspicions et aux poursuites ni celles relatives aux « litiges » soumis aux cours et tribunaux, se limitant, dans ce dernier cas, aux données relatives aux jugements civils. Dorénavant en droit belge, les banques ou grands magasins ne pourront donc plus traiter des données relatives à des suspicions de fraudes pénales.

Les exceptions au principe d'interdiction paraissent assez limitées. L'interdiction est levée si le traitement est effectué :

a) sous le contrôle d'une autorité publique ou d'un officier ministériel au sens du Code judiciaire, lorsque le traitement est nécessaire à l'exercice de leurs tâches;

b) par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance;

c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige;

d) par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige;

e) pour les nécessités de la recherche scientifique, dans le respect de conditions fixées par le Roi.

Toute personne autorisée à traiter ces données est soumise au secret professionnel. Le Roi devra fixer les conditions particulières auxquelles doivent satisfaire les traitements bénéficiant de l'exception.

3. — LES DROITS DE LA PERSONNE CONCERNÉE

3.1. — Le droit à l'information

43. — L'article 9 de la nouvelle loi regroupe en un seul article les devoirs d'information de la personne concernée mis à charge du responsable du traitement.

L'information a lieu lorsque la donnée est « obtenue » (121) auprès de la personne concernée (§ 1er) ou lorsque la donnée est obtenue auprès d'un tiers (§ 2), deux situations autrefois visées par deux articles différents, les anciens articles 4 et 9.

44. — Dans les deux situations, la loi impose une information minimale concernant ces caractéristiques, à savoir l'information sur le nom et l'adresse du responsable du traitement et les finalités du traitement. Elle ajoute une

(113) Le Conseil d'Etat critique amplement l'utilisation de ce terme, trop vague et ne se référant à aucun concept légal défini antérieurement (Avis du Conseil d'Etat, p. 220).

(114) Avis, p. 119.

(115) Exposé des motifs, pp. 38 et 39.

(116) *Idem*, p. 38.

(117) *Idem*, p. 39.

(118) Avis, p. 119.

(119) Exposé des motifs, p. 39.

(120) Sans préjudice de l'application de cette disposition pour les professionnels des soins de santé qu'elle vise.

(121) Le mot « collecte » implique une démarche active du responsable du traitement alors que l'expression « obtenir des données » vise également la situation dans laquelle la personne concernée communique spontanément les données à caractère personnel (Exposé des motifs, p. 44).

information complémentaire lorsque la finalité de marketing direct est « envisagée » par le responsable du traitement : la personne concernée doit être informée de son droit d'opposition à un tel traitement (122).

La nouvelle loi oblige désormais le responsable du traitement à fournir des informations « supplémentaires » suivant un critère déterminé par la disposition. Ces informations visent, notamment (123), les catégories de données, les catégories de destinataires, le caractère obligatoire ou non de la réponse et l'existence d'un droit d'accès et de rectification. Ces informations sont dues (124) sauf si au regard des circonstances de l'obtention des données, elles ne sont pas nécessaires pour assurer un « traitement loyal des données ». On notera que la directive utilisait une formulation inverse : ces informations n'étant dues que si elles sont nécessaires pour assurer un traitement loyal.

D'autres informations « supplémentaires » devront donc être transmises, le cas échéant, en fonction de l'application de ce critère de loyauté. Ainsi, si le traitement se déroule en partie à l'étranger, ce fait doit être révélé, au vu des risques accrus que le transfert de données implique pour la personne concernée.

Enfin, le point *e)* des §§ 1er et 2, de l'article 9 prévoit une troisième catégorie d'informations dues, celles déterminées par le Roi après avis de la Commission. Peu de précisions sont données à ce propos (125). L'exposé des motifs, se référant au considérant n° 39 de la directive, évoque des informations susceptibles d'être communiquées à un stade ultérieur à la collecte et dont la communication n'avait pas été envisagée au départ (126).

45. — On ajoutera que la nouvelle loi, pas plus que la directive ou l'ancien prescrit de l'article 4, ne prévoit des modalités particulières quant à la manière dont l'information sur les caractéristiques du traitement est transmise (127).

Le moment où l'information doit être fournie à la personne concernée diffère selon que les données sont obtenues auprès de cette dernière ou non. Dans la première situation, l'information doit lui être transmise « au plus tard au moment où ces données sont obtenues » alors que dans la seconde, l'information a lieu, au choix du responsable à qui les données ont été transférées, soit à l'enregistrement, soit si une communication à un tiers est envisagée, au plus tard lors de la première communication.

Suite à une remarque de la Commission (128), la nouvelle loi prévoit à bon escient que, dans la seconde situation, si la communication ou l'utilisation des données a lieu à des fins de marketing direct, la personne concernée doit être avertie avant la communication au tiers ou l'utilisation pour le tiers afin de pouvoir exercer en temps utile son droit d'opposition.

46. — En cas d'obtention des données auprès de la personne concernée par les données, on note que là où l'ancien article 4 n'admettait aucune exception, l'article 9, § 1er, prévoit, à la suite de la directive, la dispense du devoir d'information dans la mesure où la personne concernée est déjà informée des caractéristiques du traitement, objet du devoir d'information (129).

Si les données ne sont pas obtenues auprès de la personne concernée, deux seules exceptions au devoir d'information sont prévues.

La première vise les cas où « l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ». Le prescrit légal vise, en particulier, les traitements à finalité statistique, de recherche historique ou scientifique et ceux permettant le dépistage motivé par la protection et la promotion de la santé publique. Cela permettra sans doute de récupérer une partie des exceptions prévues par les arrêtés royaux nos 9 et 15 (130). L'avantage est ici de ne pas prévoir une longue liste de cas répondant *a priori* à ce critère. Le risque cependant est de voir les responsables s'en prévaloir automatiquement. Les contours de l'impossibilité d'information et du caractère disproportionné des efforts demandés par l'obligation d'information au responsable du traitement ne sont en effet pas clairs.

La seconde vise les cas où l'enregistrement ou la communication sont effectuées en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Son libellé élargit singulièrement la portée restreinte de l'exception prévue par la directive, sur laquelle l'exception belge prétend se fonder. La directive exige en effet en son article 11.2. que la législation prévoit expressément l'enregistrement ou la communication de données pour pouvoir bénéficier de l'exception. Ainsi, une disposition réglementaire pourrait prendre des mesures de réduction des charges de la sécurité sociale pour certaines catégories d'assujettis indépendants sur la base du montant de leurs revenus. Pour la directive, la communication des données fiscales à l'organisme de sécurité sociale devrait être prévue par la loi pour obtenir le bénéfice de l'exception au devoir d'information alors que l'assujetti belge ne sera jamais averti de cette transmission.

Le Roi est chargé de venir préciser les conditions d'application des deux exceptions.

3.2. — Les droits d'accès et d'opposition

47. — L'article 10 de la loi de 1992, est, selon la formule de l'exposé des motifs (131), « mis en conformité avec la directive européenne ». Le droit d'accès s'entend ainsi du droit d'obtenir du responsable (132) la confirmation de l'existence d'un traitement portant sur les données qui la concernent, ainsi que les informations sur les finalités du traitement, les catégories de données traitées (133) et les destinataires, la communication des données traitées, leur origine et la connaissance de la logique suivie lors du traitement (134). A ces informations prévues par la directive, la loi ajoute les renseignements quant aux diverses possibilités ouvertes à la personne concernée

(122) Sur le contenu de ce droit d'opposition, cf. *infra* n° 50. On notera que l'ancien article 4 prévoyait une information relative à l'existence du registre public.

(123) La formulation belge créera des difficultés d'interprétation dans la mesure où l'énumération des informations supplémentaires n'est pas exhaustive et que l'information supplémentaire est due.

(124) Le Conseil d'Etat (Avis du Conseil d'Etat, p. 218) rappelle qu'il s'agit d'une exception d'interprétation stricte et s'opposa avec succès à la formule plus libérale de l'avant-projet où le responsable pouvait se dispenser de l'information chaque fois que raisonnablement, il pouvait estimer que la personne était déjà informée.

(125) Ainsi, on pourrait prévoir que, dans le cas de données obtenues par le biais de cookies, le Roi oblige le responsable du site Web à informer la personne concernée de la durée d'existence de cookies et de la possibilité de bloquer leur activation.

(126) Exposé des motifs, p. 46. Ce souhait se heurte cependant au texte de l'article 9, § 1er, qui, au contraire de la directive, prévoit que l'obligation d'information s'effectue « au plus tard au moment où ces données sont obtenues », limite de temps que la directive ne prévoit pas.

(127) Le texte de l'article 9, §§ 1er et 2 de la nouvelle loi, comme celui de la directive, parle d'informations « fournies » à la personne concernée, c'est-à-dire, selon le *Petit Larousse*, d'informations qui lui sont « procurées ». Il semble donc difficile de concevoir qu'une information collective satisfasse au requis légal, alors même que la délivrance orale peut suffire.

(128) Avis, p. 14, n° 26.

(129) Il est donc à souligner que la dispense ne peut être partielle : la personne doit être informée préalablement de toutes les caractéristiques du traitement faisant l'objet du devoir d'information. La personne concernée peut savoir qu'une banque traite des données à son propos, mais ignorer les finalités du traitement, par exemple leur utilisation à des fins de marketing. Par ailleurs, l'exception ne joue que si la personne est informée, non si elle est raisonnablement supposée être informée.

(130) Arrêté royal n° 9 accordant des dispenses de l'application de l'article 9 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 et établissant une procédure d'information collective des personnes concernées par les données, *M.B.*, 28 février 1995, p. 4473; *A.R.* n° 15 modifiant l'arrêté royal n° 9, *M.B.*, 15 mars 1996, pp. 5830 et s.

(131) Exposé des motifs, p. 49.

(132) Les renseignements sont communiqués sans délais et au plus tard dans les 45 jours de la réception de la demande (art. 10, § 1er, al. 3 de la nouvelle loi); cette demande, comme sous l'ancienne loi, peut également être adressée à toute autre personne désignée par le Roi (art. 10, § 1er, al. 2 de la nouvelle loi).

(133) On retrouve clairement le risque déjà souligné auparavant de voir la personne concernée être incapable de déterminer la (les) finalité(s) exacte(s) portant sur chacune des catégories de données traitées en cas de finalités multiples et par conséquent, de contrôler l'application des principes de légitimité, de conformité et de qualités contenus dans les articles 4 et 5 de la nouvelle loi. En effet, le texte de l'article 10 parle des « catégories de données sur lequel il (*n.d.l.r.* : le traitement) porte ». La personne sait donc que différentes finalités d'utilisation portent sur certaines catégories de données. Une donnée pourrait être non pertinente pour une des finalités visées par le traitement. Si elle s'en plaint, le responsable pourrait seulement répondre que la donnée n'est pas utilisée dans ce but, sans réelle possibilité de contrôle. On ne voit donc d'autre solution que d'imposer au responsable une application des principes énoncés ci-avant à la globalité des finalités visées. Ainsi, chaque catégorie de données devrait répondre au principe d'adéquation, de pertinence, etc. à l'égard de chacune des finalités du traitement. Si tel n'est pas le cas, le traitement devrait être scindé.

(134) On notera à la suite de la Commission que cette information n'est normalement à transmettre qu'en cas de système automatisé de décision (c'est-à-dire si l'article 12*bis* est applicable). (Sur cet article, voy. *infra*, n° 52).

à la suite de cet accès (demande de correction, consultation du registre public, etc.).

Sans doute eût-il été utile d'ajouter que le droit d'accès s'exerce, comme le notait l'article 12 de la directive, « sans contrainte », c'est-à-dire en dehors de toute pression d'un tiers intéressé à obtenir via l'accès de la personne concernée, les données relatives à cette dernière.

48. — Le paragraphe 2 de l'article 10 concerne l'accès aux données relatives à la santé. Il prévoit que le droit d'accès s'exerce soit directement, soit par l'intermédiaire d'un « professionnel des soins de santé » (135). Sous certaines conditions, en matière d'utilisation de données médicales à des fins de recherches scientifiques et moyennant autorisation préalable (136) de la personne concernée pour un tel traitement, l'accès aux données peut être différé à l'issue des recherches.

49. — L'article 13 de la nouvelle loi prévoit une possibilité d'accès indirect auprès de la Commission de la protection de la vie privée en ce qui concerne les traitements dispensés du respect des articles 10 à 12 par l'article 3, §§ 4 à 6.

Les traitements effectués à des fins de sûreté de l'Etat, de sécurité publique, de défense nationale ou de prévention ou répression des infractions bénéficieront comme sous l'ancienne loi d'un régime d'accès dit « indirect ». Les auteurs de la loi justifient cette dérogation à l'article 10 par l'article 13 de la directive (137). Force est toutefois de reconnaître que l'exception dans la nouvelle loi ne répond pas au prescrit de la directive. Ce dernier prévoit, conformément à la jurisprudence de la Cour européenne des droits de l'homme, que l'exception n'est pas automatique et qu'elle doit, au vu de la particularité du traitement concerné par la demande d'accès, « constituer une mesure nécessaire pour sauvegarder » les intérêts décrits ci-dessus (138).

La référence à l'article 13 de la directive, amène à regretter que la loi belge n'ait pas cru bon reprendre un autre cas d'exception cité par cette disposition, à savoir l'hypothèse où l'accès peut entraîner un préjudice aux droits et libertés d'autrui (139). Une telle omission apparaît dommageable (140). Ainsi, un dossier de crédit, voire médical, peut contenir des références à des données personnelles concernant d'autres membres de la famille. Devait-on admettre, comme l'impose la nouvelle loi, que ces autres membres puissent exercer leur droit d'accès au seul motif que le traitement contienne des renseignements à leur propos?

50. — L'article 12, § 1er, de la nouvelle loi consacre le droit d'opposition dans deux hypothèses.

La personne concernée a désormais le droit de s'opposer au traitement de certaines de ses données pour des raisons sérieuses et légitimes tenant à une situation particulière. L'opposition ne porte que sur les données. Ainsi, si les résultats scolaires d'un étudiant peuvent légitimement être communiqués par l'école secondaire à l'université, cet étudiant peut s'opposer non à la communication en tant que telle, mais à la communication d'une donnée particulière : doublement d'une année dû à des circonstances familiales difficiles dans la mesure où cette information pourrait lui être préjudiciable. Conformément à la possibilité laissée par l'article 14 de la directive, la loi interdit ce droit d'opposition lorsque le traitement est nécessaire à la conclusion ou à l'exécution d'un contrat ainsi qu'au respect d'une obligation légale (141).

L'autre hypothèse d'opposition est plus novatrice (142). Gratuitement et sans justification, la personne concernée peut s'opposer au traitement projeté lorsque des données à caractère personnel sont collectées à des fins de marketing direct. On rappellera par ailleurs que l'article 9, § 2, *c*, impose désormais à la personne responsable une obligation préalable d'informer la personne concernée, lorsque la première entend communiquer des données relatives à la seconde à des tiers ou les utiliser pour des tiers à des fins de marketing direct. Ainsi, l'opposition au traitement à des fins de marketing direct peut s'opérer dans deux hypothèses :

— soit le responsable du traitement effectue lui-même la collecte, il doit alors offrir lors de cette collecte la possibilité de s'opposer gratuitement au traitement;

— soit celui au bénéfice duquel le traitement à des fins de marketing est projeté, tantôt utilise les services d'un responsable de traitement, tantôt demande à ce dernier communication des données : dans cette double hypothèse, le responsable est tenu d'informer suivant l'article 9, § 2, *c*, la personne concernée de son droit d'opposition à l'utilisation ou à la communication envisagée.

51. — L'article 12, § 3, de la loi est également modifié. La rectification des données contestées est communiquée par le responsable du traitement dans le mois de la demande tant à la personne concernée (143), qu'aux tiers auxquels les données ont été communiquées. Ces derniers ne reçoivent la rectification que « pour autant que le responsable du traitement ait encore connaissance des destinataires de la communication » — ce que prévoyait déjà l'ancien article 12, § 3 — et que « la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés », seule hypothèse prévue par l'article 12 de la directive.

Le cumul de l'exception ancienne et de celle prévue par la directive apparaît non conforme à la volonté européenne qui précisément faisait obligation au responsable, dans toute la mesure du possible, et ce au vu des risques de dommages susceptibles d'être subis par la personne concernée, de conserver l'identité des tiers auxquels l'information est communiquée.

(135) L'alinéa 2, formulé sur proposition de la Commission (Avis, p. 17, n° 31), permet que dans ce cas, le responsable sollicité puisse imposer que l'accès soit réalisé par un professionnel de la santé choisi par la personne concernée. La Commission préféra cette formulation à celle où le responsable pouvait refuser l'accès si l'information était susceptible de nuire gravement à la santé de la personne concernée. Elle craignait que le responsable ne s'abrite trop facilement derrière cette exception. Il n'est pas certain que la nouvelle formulation proposée par la Commission atteigne le but d'une plus grande transparence médicale dans la mesure où le responsable pourra exiger l'accès indirect dans tous les cas. A cet égard, on aurait pu imaginer que le refus d'accès direct soit motivé, de manière purement interne, par le fait que cet accès risque de nuire gravement à la santé de la personne concernée. Par ailleurs, seul un médecin pourra, selon nous, être choisi pour accéder à des données couvertes par le secret professionnel et non tout professionnel de la santé (simple infirmier ou pharmacien) comme le texte pourrait le laisser croire. Le problème du droit d'accès au dossier médical fait l'objet de dispositions dans le cadre de l'avant-projet de loi dit Colla modifiant la loi sur les hôpitaux, coordonnée le 7 août 1987 et de l'A.R., n° 78 du 10 novembre 1967, relatif à l'exercice de l'art de guérir, de l'art infirmier, des professions paramédicales et aux commissions médicales.

(136) Cette condition a été ajoutée à la demande du Conseil d'Etat. Pour une critique du libellé du § 2, jugé trop restrictif, et de manière plus générale pour une analyse de droit comparé des questions de protection des données personnelles en matière de santé et les besoins de la recherche scientifique, lire l'étude de Jan Dhont et Y. Poullet, *De verwerking van medische persoonsgegevens voor statistische en medische doeleinden*, 1998, SSTC, Bruxelles, 105 pages.

(137) Cf. le tableau comparatif repris en annexe du projet de loi (Doc. 1566/2 - 1997-1998, Ch. rep., sess. ord. 1997-1998, 20 mai 1998, p. 70).

(138) A ce propos, lire Y. Poullet, B. Havelange, *op. cit.* Les auteurs y défendent un système d'accès direct avec possibilité pour les organismes visés d'un refus motivé et, dans ce dernier cas, d'un accès indirect par un intermédiaire comme la Commission de protection de la vie privée.

(139) La Commission (Avis n° 32) s'était opposée à l'ajout de cette exception considérée comme trop floue. Le Conseil d'Etat (Avis du Conseil d'Etat, p. 195) tout en reconnaissant l'intérêt d'une telle restriction avait souhaité que l'exception soit limitée aux « droits et libertés des tiers » et que le « législateur détermine avec une relative précision, les cas où cette protection s'impose, et quand elle s'oppose à l'exercice des droits normalement reconnus ». Le représentant du ministre devait finalement abandonner cette restriction sans chercher à la préciser, suite à un amendement voté en Commission de la justice (Rapport, pp. 80 et 81).

(140) Ainsi, comme le notait le Conseil d'Etat (*eod. loc.*) et le représentant du ministre (Exposé des motifs, p. 25) : « Il est en effet possible que dans certaines circonstances, le droit d'accès ne peut être exercé totalement ou partiellement sans mettre en péril la vie privée d'une autre personne, par exemple lorsque l'information relative à la personne concernée est indissolublement liée à des informations relatives à un tiers » (cf. à cet égard, l'exemple de la collecte par un travailleur social de données relative à la personne concernée auprès de la famille de celle-ci, Rapport, p. 80).

(141) Le droit d'opposition pourrait pourtant se justifier dans les deux cas exemptés. Ainsi, en matière de crédits à la consommation, la communication d'un défaut de paiement de la banque aux centrales est prévue par la loi. On peut cependant imaginer que pour des raisons particulières, la personne concernée puisse s'opposer légitimement à une telle communication.

(142) Encore que dans les faits, les entreprises de marketing direct avaient déjà créé une liste Robinson reprenant l'identité des personnes s'opposant à la réception d'offres individualisées (cf. à cet égard, le code de déontologie de l'Association belge du marketing direct) et que la Commission de protection de la vie privée avait, dans quelques recommandations ou avis, préconisé ce droit d'opposition.

(143) L'ancienne disposition avait omis cette précision.

3.3. — La non-soumission à des décisions individuelles automatisées

52. — L'article 12*bis* de la nouvelle loi interdit qu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative soit prise « sur le seul fondement » d'un traitement automatisé destiné à évaluer certains aspects de sa personnalité. L'article 15 de la directive vise au premier chef les systèmes automatisés évaluant le rendement professionnel, le crédit, la fiabilité et le comportement de la personne concernée. L'exposé des motifs précise que « cette disposition doit éviter que, sans aucune intervention humaine, des décisions sont prises directement sur la base d'un résultat d'un traitement automatisé » (144).

Deux exceptions sont prévues à l'alinéa 2 de l'article 12*bis*. La première exception vise les décisions prises dans le cadre d'un contrat (145). La seconde exception permet la décision automatisée fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance (146). Le contrat et la disposition légale ou réglementaire doivent contenir des mesures appropriées garantissant la sauvegarde des intérêts légitimes de la personne concernée. Nulle précision n'est cependant donnée à cet égard. On peut imaginer que de simples mesures de vérification de qualité lors de l'introduction des données pourraient suffire. La personne concernée doit se voir au moins autoriser — selon le prescrit légal — à faire valoir « utilement » son point de vue.

53. — Que conclure de cette analyse des dispositions relatives aux droits de la personne concernée et de leur transposition de la directive? Indiscutablement, la loi consacre un renforcement de tels droits. La création de nouveaux droits comme celui d'opposition ou celui de ne point être soumis à une décision fondée sur le seul résultat d'un traitement automatisé en constitue une première manifestation. On peut souligner aussi l'élargissement de l'obligation d'informer mise à charge du responsable du traitement vis-à-vis de la personne concernée. Enfin, le nombre d'informations auxquelles la personne concernée a accès s'est accru.

Par contre, la loi n'utilise pas, loin s'en faut, les multiples exceptions générales et nuances suggérées par la directive, notamment en son article 13, même si certaines exceptions sont créées pour certaines administrations publiques ou dans des hypothèses parfois contestables.

4. — LE CONTRÔLE DES TRAITEMENTS

54. — Plusieurs points de vue peuvent être adoptés en la matière : on distinguera le contrôle interne du contrôle externe. Le contrôle interne consiste dans les mesures organisationnelles techniques et autres que le responsable du traitement peut prendre au sein de son organisme pour assurer le respect des prescrits légaux. Le contrôle externe envisage les divers modes d'inspections, de recours et de sanctions que des autorités externes au responsable du traitement peuvent prendre sur demande ou d'initiative pour s'assurer du respect de tels prescrits.

En ce qui concerne le contrôle externe, celui-ci peut s'exercer *a priori* ou *a posteriori*. La déclaration d'un traitement, l'avis préalable de la Commission peuvent ainsi apparaître comme relevant des contrôles de la première catégorie à l'inverse des recours administratifs et juridictionnels exercés une fois le traitement mis en place.

Par rapport aux législations existantes et, en particulier, à l'ancienne législation belge, la directive traduit la volonté d'un renforcement des modes de contrôle interne et en ce qui concerne le contrôle externe, notamment à propos des compétences de l'autorité de contrôle, un glissement des formes de contrôle *a priori* vers des formes de contrôle *a posteriori* (147).

4.1. — Le contrôle interne

55. — L'ancienne loi consacrait en son article 16/1 l'obligation du responsable de prendre un certain nombre de mesures de sécurité. Elle-même inspirée du texte en projet de la directive, cette disposition n'a pas fait l'objet de grands changements.

L'obligation de sécurité est maintenue en des termes quasi identiques, mais elle doit être respectée également par le sous-traitant (148).

Le paragraphe premier prescrit les conditions sous lesquelles les traitements peuvent être confiés à des sous-traitants. Ces derniers doivent apporter des garanties suffisantes quant à la sécurité et le responsable doit veiller au respect de ces mesures. Un contrat doit fixer la responsabilité du sous-traitant et prévoir que ce dernier n'agit que sur la seule instruction du responsable (149). Toute personne qui a accès aux données à caractère personnel, agissant sous l'autorité du responsable ou du sous-traitant — ainsi que le sous-traitant lui-même —, ne peut traiter les données que sur instructions du responsable du traitement (150).

56. — L'ancienne loi prescrivait en outre le devoir du responsable de maintenir un « état » pour chaque traitement. Il s'agissait d'un document décrivant de manière complète et détaillée les caractéristiques du traitement et la manière dont il s'insérait dans le système d'informations de l'organisation, de l'entreprise ou de l'administration (interconnexions, rapprochements de données, destinataires, modes d'accès, ...).

Cet « état » au contenu plus précis que celui de la déclaration poursuivait un double objectif. Le premier était certes d'assurer la transparence interne des flux d'informations et des opérations pratiquées sur ces dernières. Le second, celui de permettre aux contrôleurs externes, la Commission de protection de la vie privée ou le juge, d'avoir une vue complète du système d'informations détenu par le responsable. Le législateur abandonne cette mesure de contrôle interne au double motif léger du non-respect dans la réalité de cette obligation et du double emploi que cette mesure constitue avec celle de la notification (151). L'abandon de cette obligation de tenir en état est regrettable au moment même où se multiplient les possibilités de dispense de déclaration préalable.

(144) Exposé des motifs, p. 17 qui précise en outre que « On respecte donc la disposition lorsque, entre l'obtention du résultat du traitement par ordinateur et la prise de décision, il y ait au moins une intervention humaine minimale ». L'interdiction vaut donc non seulement lorsqu'il n'y a aucune intervention humaine mais également lorsque la décision est transmise par l'intermédiaire d'une personne sur la seule base du résultat du traitement. L'intervention humaine doit donc avoir pour conséquence la prise en compte d'autres éléments que les résultats du traitement. En pratique, la charge de la preuve pèsera sur la personne concernée par les données. Elle sera aidée par le fait que l'accès porte également sur la logique qui sous-tend le traitement (voy. *supra*, n° 47). On peut se demander également si la logique du raisonnement qui sous-tend la décision prise sur la base non exclusive du traitement ne devrait pas être expliquée à la personne concernée sur la base de l'obligation d'information. Sans cela, on peut craindre que la personne concernée ait de sérieuses difficultés à prouver que les conditions d'application de la disposition sont remplies.

(145) Les crédits-scoring et les systèmes d'évaluation de la rentabilité de travailleurs pourraient donc bénéficier de l'exception.

(146) La seconde exception laisse ainsi la porte ouverte à la création de systèmes experts dans les administrations fiscales, de sécurité sociale, de santé, fondés sur des simples arrêtés pris en vertu d'une loi, ce qui pose la question de la compatibilité de la présente disposition avec l'article 22 de la Constitution. En outre la directive exige que la décision automatisée soit « autorisée » par la loi. Il ne suffit donc pas qu'une prise de décision soit nécessaire pour appliquer la loi ou le règlement. Il faut que ces derniers autorisent la prise de décision automatisée.

(147) Sur la démonstration de ce point de vue, le lecteur voudra bien se référer à Y. Poullet, « L'autorité de contrôle : "Vues" de Bruxelles, *Rev. franç. dr. adm.*, 1999, *in* n° spécial : « La protection des données », en cours de publication.

(148) Article 16, § 4, de la nouvelle loi.

(149) L'article 16, § 1er, 4°, de la nouvelle loi impose également aux parties de convenir que le sous-traitant doit respecter l'obligation de sécurité prévue au paragraphe 4 de la disposition. Le non-respect de l'obligation légale de sécurité par le sous-traitant devra donc être considéré comme une violation du contrat le liant au responsable du traitement. Si le responsable n'a pas prévu une telle clause dans le contrat, il commet lui-même une violation de la loi.

(150) Article 16, § 3, de la nouvelle loi. A noter le double effet de cette disposition : premièrement, elle impose aux employés un devoir de confidentialité et de respect des instructions de l'employeur et rend l'employé coupable d'infraction contractuelle (envers l'employeur), délictuelle voire pénale (envers la personne concernée) en cas de non-respect de telles instructions; secondement, elle oblige le responsable (c'est-à-dire les organes habilités de l'entreprise ou de l'administration) à prendre de telles instructions. Tout défaut de prise de telles mesures constitue une violation de la loi par le responsable du traitement.

(151) Exposé des motifs, p. 54. L'avis de la Commission (Avis, n° 42) reprenait les arguments du gouvernement. La Commission notait cependant que certaines informations non présentes dans la déclaration étaient reprises dans l'« état », telle la liste des destinataires. Sur ce point précis, le gouvernement devait par la suite ajouter, la mention des destinataires dans le contenu de la déclaration, ce que la directive lui imposait d'ailleurs.

57. — Comme condition de simplification ou de dérogation à l'obligation de déclaration, la directive prévoit une autre mesure de contrôle interne, reprise de l'expérience allemande (152), la nomination d'un « détaché à la protection des données » (153), personne « indépendante » chargée de veiller au respect des prescrits de la directive et de tenir un registre correspondant plus ou moins à l'état dont nous venons de parler. L'intention de la directive était, par cette possibilité et la faveur qui lui était attachée, de favoriser l'émergence d'une nouvelle fonction au sein des entreprises ou des administrations. L'intérêt était double : assurer un contrôle interne et faciliter le contrôle externe dans la mesure où le dialogue avec une personne attachée aux mêmes valeurs devait en principe faciliter la tâche du contrôleur externe.

La nouvelle loi (154) prévoit bien la création d'un « préposé » (155) à la protection des données mais uniquement dans les hypothèses de traitements « qui présentent des risques particuliers » et ce n'est que sur l'insistance du Conseil d'Etat (156) à voir fixer par la loi la mission et le statut de ce préposé, que, *in fine*, le gouvernement proposa de réserver ce soin au Roi. Ce faisant, loin de voir, comme dans la directive, l'institution servir comme solution à un allégement des charges administratives imposées au responsable du traitement, la loi l'utilise comme un instrument supplémentaire de contrôle de ce dernier. Par là, elle manque une occasion d'introduire en droit belge un substitut simple et pratique à l'obligation de déclaration.

4.2. — Le contrôle externe

4.2.1. — *Le contrôle spécialisé : la Commission de protection de la vie privée*

58. — La directive baptise cet organe « autorité de contrôle », affirmant d'emblée le pouvoir effectif d'intervention de cette autorité et non plus simplement le simple pouvoir d'avis ou de recommandation qui lui était traditionnellement reconnu en particulier, mais non uniquement, en Belgique. Par ailleurs, si la directive reconnaît à cette autorité un rôle préventif plus réduit, elle augmente résolument son pouvoir d'intervention *a posteriori*.

La loi belge semble sourde aux accents nouveaux de la directive. Elle modifie peu les instruments de contrôle, les compétences et la composition de la Commission. Elle redéfinit par ailleurs les relations de la Commission avec les comités sectoriels (157).

4.2.1.1. — *L'instrument de contrôle : la déclaration*

59. — L'instrument de contrôle de la Commission est traditionnellement la déclaration qui lui permet de s'assurer de la conformité du ou des traitements déclarés vis-à-vis des principes de la loi. La directive modifie peu le régime des déclarations actuelles et dès lors l'article 17 ne fait l'objet que d'adaptations mineures.

60. — La première modification concerne l'objet même de la déclaration.

L'obligation de déclaration porte — énonce l'article 17, § 1er, de la loi — sur tout « traitement entièrement ou partiellement automatisé ou d'un ensemble de tels traitements ayant une même finalité ou des finalités liées ». On a vu qu'un seul traitement pouvait poursuivre plusieurs finalités. On a également indiqué que les données devaient être traitées de manière compatible avec ces finalités ce qui imposait un critère de « compatibilité » entre les finalités poursuivies par le traitement. Le législateur indique en outre — dans la disposition commentée — que des finalités de différents traitements peuvent être « liées ». Que faut-il comprendre par là?

Le paragraphe 5 de l'article 17 précise en outre que : « Chaque finalité ou un ensemble de finalités liées pour lesquelles il est procédé à un ou plusieurs traitements partiellement ou totalement automatisés doit faire l'objet d'une déclaration ». La règle est plus qu'ambiguë. La liaison entre finalités porte-t-elle sur les finalités d'un même traitement ou sur les finalités poursuivies par différents traitements? L'article 17, § 1er, implique que seule la seconde interprétation soit retenue. L'article 17, § 3, 5°, de la nouvelle loi mentionne par contre, parmi les informations contenues dans la déclaration, « la finalité ou l'ensemble des finalités liées du traitement automatisé ». Cette dernière disposition impliquerait donc que la liaison dont question vise les finalités d'un même traitement. Une contradiction apparaît entre les trois dispositions.

L'exposé des motifs n'aide pas à la compréhension. La déclaration, d'après lui (158), concernait, sous l'empire de l'ancienne loi, un traitement, c'est-à-dire à un ensemble d'opérations correspondant à une seule finalité précise. Chacun des traitements devant être déclaré, on en arrivait à l'équation « un traitement = une finalité = une déclaration ». Sur la base d'une interprétation erronée de la directive, remettant en cause la notion même de traitement (159), l'exposé conclut que désormais ce n'est pas le traitement qui est l'objet de la déclaration mais « les finalités éventuellement liées par lesquelles un ou plusieurs traitements sont effectués » (160). Un traitement

(152) Sur l'expérience allemande des « Datenschutzbeauftragte » et leur statut, lire Y. Poullet, *in* J. Hubin et Y. Poullet, « L'obligation de sécurité dans les législations de protection des données », *in La sécurité informatique : aspects techniques et juridiques*, Diegem-Namur, Story-Scientia-C.R.I.D., *Cahiers du C.R.I.D.*, n° 14, 1998, pp. 215 et s. La mesure de nomination d'un préposé permet de favoriser une culture de protection des données, interne à l'entreprise ou à l'administration. Dans le cas de p.m.e., on peut envisager que le rôle de préposé soit confié à des organismes externes comme des sociétés d'audit ou des chambres de commerce et d'industrie qui pourraient assurer pour plusieurs entreprises la tâche dévolue au préposé; voy. aussi « La protection des données à caractère personnel en droit communautaire », p. 153, n° 64.

(153)... à la protection des données et non à la sécurité dans la mesure où la sécurité est un concept plus large que celui de la protection des données et peut inclure la lutte contre les pannes, la protection des investissements et des secrets d'affaires de l'entreprise, ce qui peut écarter, la personne préposée à la sécurité du souci premier de protection des données.

(154) Article 17*bis* de la nouvelle loi.

(155) Le terme « détaché » évoque plus que celui de « préposé » l'autonomie dont doit disposer ce contrôleur interne par rapport à sa hiérarchie.

(156) Avis du Conseil d'Etat, p. 232. Le Conseil d'Etat excluait la compétence du Roi de fixer le statut et la mission du préposé dans la mesure où la matière de la vie privée concernée par l'article 22, al. 2, l'exige. Il est à noter, que dans une première version, le projet de loi prévoyait une dispense de déclaration lorsqu'un préposé était nommé mais « ce plan a été abandonné. Il est non seulement pratiquement impossible d'élaborer au niveau de la loi un statut pour un tel préposé, valable pour toutes les situations, mais en plus il n'apparaît pas opportun de lier la désignation d'un préposé à une exemption à l'obligation de déclaration » (Exposé des motifs, p. 56). Curieusement, on notera que pour les traitements du « Centre européen pour enfants disparus » bénéficiaires selon l'article 3, § 6, de nombreuses exceptions à l'application de la loi, celle-ci prévoit la désignation « parmi les membres du personnel du Centre d'un préposé à la protection des données ayant connaissance de la gestion et de la protection des données à caractère personnel. L'exercice de ses missions ne peut entraîner pour le préposé des désavantages. Il ne peut en particulier, être licencié ou remplacé comme préposé à cause de l'exécution des tâches qui lui sont confiées... » En d'autres termes, ne pouvait-on simplement étendre ces principes à tous les « préposés »?

(157) Ce dernier point ne pourra être évoqué dans le cadre du présent article.

(158) Exposé des motifs, p. 55.

(159) *Idem* : « La directive utilise une série de notions plus précises. Un traitement est, comme dans le langage usuel, défini comme toute opération effectuée avec des données à caractère personnel. Au sens de la directive, il arrive donc souvent que de très nombreux traitements soient effectués pour la même finalité. L'obligation de déclarer ne concerne pas les traitements séparés mais les finalités pour lesquelles un ou plusieurs traitements sont effectués ». Ce raisonnement est incorrect. La directive, on l'a vu, permet effectivement qu'à un traitement corresponde plusieurs finalités. Une opération portant sur les données ou un ensemble d'opérations est constitutif d'un traitement. Il n'en reste pas moins que la finalité ou les finalités poursuivies restent l'élément unificateur du traitement. La directive ne considère cependant pas que chacune des opérations doit être considérée automatiquement comme un traitement. Si tel était le cas, cette notion deviendrait superflue. Une opération devient un traitement lorsqu'elle est transcendée par une finalité d'utilisation propre par celui qui la poursuit. Ainsi, la collecte ou la consultation pourraient être constitutifs d'un traitement dans le chef de celui qui effectue ces opérations en l'absence même d'aucune autre opération subséquente. Si les finalités qu'il poursuit imposent d'autres opérations sur les données, « l'ensemble » de ces opérations constitue le traitement poursuivi.

(160) Le raisonnement tenu par le gouvernement lui permettra de justifier l'abandon de l'obligation pour le responsable du traitement de déclarer le « numéro de traitement » sur toute pièce qui en matérialise l'usage. Le Conseil d'Etat (p. 235) avait réclamé le maintien de cette obligation prévue par l'article 18, alinéa 4, de la loi de 1992, en arguant de l'intérêt que ce « numéro » présente pour la personne concernée qui peut vérifier que le traitement a bien été déclaré et dès lors, le cas échéant, le contenu de la déclaration. L'exposé des motifs se contente d'affirmer que « l'avis du Conseil d'Etat ne peut pas être suivi parce qu'il est basé sur l'opinion fautive que la déclaration se fait au niveau du (simple) traitement » (Exposé des motifs, p. 57). Si l'obligation prévue par l'ancien article 18 avait pu apparaître lourde et inutile, elle aurait pu présenter, dans certains cas, en particulier pour les traitements de marketing direct et ceux effectués par les sites Web, une manière aisée pour les personnes concernées de s'assurer du contenu de la notification et en particulier de l'identité du responsable du traitement.

pourrait donc faire l'objet de plusieurs déclarations si les finalités ne sont pas liées. Différents traitements pourraient aussi faire l'objet d'une seule déclaration si les finalités poursuivies par les deux traitements sont liées.

On en arrive à une situation incompréhensible et inextricable. Une interprétation utile de tous ces textes contradictoires doit donc être recherchée. On pense qu'il est bon ici d'éviter deux écueils. La seule détermination de l'objet de l'obligation de déclaration ne peut être la justification d'une interprétation nouvelle des concepts de base de la loi. En outre, la déclaration doit remplir le but de transparence, qui lui a toujours été assigné et permettre à la Commission d'effectuer un contrôle efficace.

L'article 17, § 1er, reprend le principe général de l'ancienne loi : « Préalablement à la mise en œuvre d'un traitement automatisé (...) le responsable du traitement (...) en fait la déclaration (...) ». Si le traitement poursuit une seule finalité, la situation est identique à celle vécu sous l'ancienne loi. Si ce traitement poursuit différentes finalités, elles doivent être compatibles au sens indiqué ci-avant. C'est la liaison qui pourrait être visée par l'article 17, § 5, de la nouvelle loi. La déclaration indique alors les différentes catégories de données traitées et les finalités du traitement qui les transcendent, de sorte que tant la personne concernée, que la Commission puissent déterminer le lien existant entre chaque catégorie de données et chacune des finalités. Un contrôle effectif, suite à la modification de la notion de traitement, est à ce prix. Si ces finalités sont incompatibles ou non liées, il s'agit en fait de différents traitements qui doivent donner lieu à différentes déclarations.

Permettant l'allégement du système de déclaration, l'article 17, § 1er, énonce en outre une règle particulière : un ensemble de traitements ayant une même finalité ou des finalités liées peuvent faire l'objet d'une seule déclaration. On vise ici à permettre au responsable qui poursuit plusieurs traitements différents, de grouper ceux-ci dans une seule déclaration. Il faut toutefois que les finalités de ces différents traitements soient identiques ou soient liées. Dans la première hypothèse, on peut penser à une entreprise centralisant les traitements relatifs à l'administration du personnel de diverses sociétés du même groupe. Elle ne va pas déclarer autant de traitements qu'il existe d'entreprises concernées. Les finalités des différents traitements sont uniques. Une seule déclaration suffira. Dans la seconde hypothèse, on peut penser à deux traitements, dont l'un poursuit une finalité d'administration du personnel et l'autre, la gestion des salaires de ce personnel. Les finalités d'utilisations sont distinctes. Les données nécessaires à l'un ne sont pas identiques à celles nécessaires à l'autre. Les contrôles de légitimité des finalités, de conformité et de qualité des données s'opèrent de manière distincte. Elles sont néanmoins liées : elles concernent des données relatives aux même personnes, traitées par un même responsable, visent à gérer la relation entre le responsable et les personnes qui travaillent sous son autorité, etc. Bref, les circonstances de fait seront déterminantes : elles doivent démontrer une parenté évidente entre les finalités des deux traitements et l'absence de risque particulier déduit de l'absence de déclarations distinctes (161).

Il reste encore à déterminer les limites de la « liaison » acceptée entre les finalités des traitements pouvant faire l'objet d'une seule et même déclaration. Le paragraphe 5 de l'article 17 charge la Commission de déterminer la nature et la structure de la déclaration. Il lui reviendra donc de déterminer précisément les hypothèses où cette déclaration unique pourra être acceptée. Elle pourra être guidée par la nécessité d'éviter les écueils mentionnés ci-avant. En toute hypothèse, les finalités de chacun des traitements devront être distinguées en application de l'article 17, § 3, 5° (162).

Les informations contenues dans la déclaration ont été quelque peu modifiées à la suite de la directive, l'origine des données et la technique d'automatisation choisie ne sont plus requises (163) et, désormais, devra être communiquée une description générale des mesures de sécurité.

61. — La nouvelle loi reprend une seule des deux possibilités d'exemption proposées par la directive (164), c'est-à-dire lorsqu'il n'y a manifestement pas de risques d'atteinte aux droits et libertés des personnes concernées (165). A noter que l'exemption oblige les responsables de traitements dispensés à fournir les informations, objets de la déclaration, à toute personne qui en fait la demande.

A l'inverse de ce régime d'exemption, à l'adresse de traitements présentant des risques particuliers en fonction de catégories fixées par le Roi, des conditions particulières pour garantir les droits et libertés de la personne sont prévues par le nouvel article 17*bis*.

4.2.1.2. — *Les compétences de la Commission*

62. — L'article 28 de la directive élargit singulièrement les compétences de l'autorité de contrôle. En particulier, il double les pouvoirs d'investigation de la Commission, de pouvoirs effectifs d'intervention y compris le « pouvoir d'ordonner l'effacement ou la destruction des données ou d'interdire temporairement ou définitivement un traitement » et du « pouvoir d'ester en justice ». Ce n'est pas le lieu de reprendre ici la démonstration faite ailleurs (166) de la manière dont ce renforcement de l'autorité a été traduit dans les premières législations (Royaume-Uni, Suède, Grèce, Italie, Portugal) ayant transposé la directive mais de constater que la nouvelle loi belge ne semble pas avoir suivi le mouvement.

Certes, il est prévu par le nouvel article 19 un pouvoir d'injonction de la Commission pour obtenir les informations faisant objet de la déclaration. Cette modification mise à part, la Commission ne sort pas renforcée de la nouvelle mouture légale même si elle conserve ses prérogatives antérieures de recommandations et de dénonciations en justice. La seule réelle nouveauté est sans doute la compétence de la Commission attribuée par l'article 44 de la loi en matière d'homologation (167) des codes de conduite produits par les associations professionnelles.

Toujours à ce propos et dans le même sens, on ajoutera que l'indépendance budgétaire et l'autonomie dans le choix des membres de son secrétariat, réclamés par la Commission, n'ont pas été accordées (168).

4.2.1.3. — *La composition de la Commission*

63. — Sur ce point également, la loi n'apporte guère de modifications importantes au régime antérieur. Ainsi, il n'a pas été jugé utile de reprendre les remarques opportunes du Conseil d'Etat qui, à propos de l'indépendance des membres de la Commission, se demandait si « une partie au moins des membres de la Commission aurait à être élue à cette fonction en dehors de toute présentation par le conseil des ministres » (169).

4.2.2. — *Les autorités administratives et juridictionnelles*

64. — L'article 22 de la directive prévoit la possibilité pour les Etats membres d'organiser un recours administratif notamment devant les autorités de contrôle avant la saisine des juridictions, qu'elles soient d'ordre judi-

(161) Pour reprendre l'exemple précité, une p.m.e. de 40 ouvriers pourra normalement affirmer que ses traitements « administration du personnel » et « gestion des salaires » poursuivent des finalités liées mais une grosse entreprise qui utilise des systèmes sophistiqués de calcul de la rentabilité de son personnel devra considérer les traitements « administration de personnel » et « gestion des salaires » comme poursuivant des finalités non liées et par conséquent devra introduire deux déclarations.

(162) Cette discussion n'est pas purement théorique puisqu'elle justifie aux yeux du gouvernement le fait que la déclaration n'étant plus liée au traitement, il est désormais impensable d'exiger que le responsable du traitement fasse figurer « le numéro du traitement sur toute pièce qui en matérialisera l'usage » (cf. *supra*, note 160).

(163) On note que la Commission peut toujours réclamer ces informations complémentaires.

(164) L'autre possibilité était celle liée à la nomination d'un détaché à la protection des données.

(165) La liste des traitements exemptés est dressée par le Roi, cette fois non plus sur proposition ou avis de la Commission comme c'était le cas sous l'empire de la loi ancienne, mais après avis de celle-ci.

(166) Y. Poullet, « L'autorité de contrôle : "Vues" de Bruxelles », *op. cit.*

(167) Cette compétence est prévue par l'article 27 de la directive. Selon l'expression de la loi, « la Commission s'assure en particulier que les projets qui lui sont soumis sont conformes à l'exécution de la présente loi et de ses mesures d'exécution et examine, dans la mesure du possible, les positions des personnes concernées ou de leurs représentants ».

(168) Avis, n° 59 : « La Commission, si elle veut relever de tels défis, se doit d'être efficace, donc forte et donc maîtresse d'elle-même. Ceci suppose tout d'abord une Commission plus indépendante disposant de moyens budgétaires et administratifs nécessaires. A cet égard, la Commission déplore la situation actuelle qu'en fait un des services du ministère de la Justice sur le plan financier et de l'administration. Cette situation l'empêche de pouvoir sélectionner les candidats aux postes vacants de manière autonome... ».

(169) Avis du Conseil d'Etat, p. 240. A ce propos, le Conseil d'Etat (p. 241) qui, se référant à l'arrêt *Klass c. R.F.A.* du 6 septembre 1978, arrêt qui soulignait l'importance de la représentation en ce compris de l'opposition, énonce : « Le droit exclusif de présentation conféré au pouvoir exécutif et la logique majoritaire qui le sous-tend, ne sont pas en parfaite harmonie avec la nature des missions précitées ».

ciaire, administrative ou constitutionnelle. Ce recours juridictionnel doit être offert obligatoirement. Conformément à sa volonté de ne pas accroître les compétences de la Commission, la loi ne saisit pas cette opportunité de transformer la Commission en chambre de recours (170) dont la saisine serait préalable à un recours juridictionnel (171).

65. — L'article 23 de la directive reconnaît le droit de la personne concernée d'obtenir du responsable la réparation des dommages subis « du fait » d'un traitement illicite ou en violation des dispositions prises en exécution de la directive. La possibilité d'une exonération totale ou partielle du responsable au cas où il démontre la non-imputabilité du fait qui a provoqué le dommage est affirmée par l'alinéa 2 du même article. L'article 15*bis* de la nouvelle loi reprend le principe de la directive mais l'exprime en des termes différents : « le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi. Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable ».

Le Conseil d'Etat voit dans le système de la directive, un système analogue à celui retenu par le droit français en cas de violation d'une obligation contractuelle de résultat (172). L'exposé des motifs parle quant à lui « d'une forme légère de responsabilité objective » (173). En effet, la personne concernée qui se prétend victime d'un dommage doit seulement démontrer, outre la réalité de son dommage, l'acte contraire à la loi ou à ses arrêtés d'application. Elle ne doit par contre pas démontrer la faute du responsable du traitement. Le responsable ne pourra s'exonérer que s'il prouve dans un premier temps la réalité du fait qui a provoqué le dommage et dans un second temps que ce fait ne lui est pas imputable (174).

(170) Il est à noter que la directive (art. 28, § 4) prévoit que le recours devant l'autorité de contrôle peut être le fait de la personne concernée ou d'une organisation la représentant, ce qui n'est pas le cas en Belgique dans le cadre de l'action prévue par l'article 14 de la loi belge ni même d'ailleurs devant la Commission. Cette remarque conduit à estimer que le droit de la personne concernée à être assistée lors d'un recours contre un responsable du traitement est insuffisamment reconnu en Belgique.

(171) La loi ne modifie en rien les compétences attribuées au président du tribunal de première instance statuant comme en référé; l'article 14 de la loi du 8 décembre 1992 est maintenu intégralement.

(172) Avis du Conseil d'Etat, p. 227.

(173) Exposé des motifs, p. 53.

(174) Ainsi, l'enregistrement par une banque d'un défaut de paiement qui lui a été signalé par la Banque nationale peut conduire au refus d'un prêt. A supposer cette donnée erronée et jugée cause de refus du prêt, la banque peut démontrer que la cause du dommage est imputable à la faute d'un tiers, la Banque nationale, voire la personne concernée elle-même qui, avertie par la Banque de l'enregistrement et des conséquences de celui-ci, n'a point protesté. Le raisonnement serait-il le même si la donnée erronée avait conduit à un prêt à des conditions plus onéreuses et non au refus du crédit? Peut-on considérer que dans ce cas, il y a atteinte à la vie privée et à la liberté d'obtenir du crédit? Tout dépend de la portée que l'on reconnaît à la loi. S'agit-il simplement de protéger les libertés des individus ou, au-delà, de reconnaître le droit de chacun à voir respecter, son image informationnelle?

Si la démonstration de l'acte contraire peut être facile lorsque la disposition légale ou réglementaire ne souffre d'aucune interprétation possible — p. ex. la déclaration n'a pas été introduite — elle sera souvent difficile lorsque la disposition légale — comme en matière de sécurité des traitements, de mise à jour de pertinence et de qualité des données — requiert la nécessaire interprétation du juge. Sur ce plan, le responsable du traitement pourra se défendre : les mesures prises en matière de sécurité correspondaient aux exigences légales et la pertinence des données pouvait être légitimement appréciée dans le sens suivi et contesté par la personne concernée.

Plus difficile encore, il incombe à la personne concernée d'apporter la preuve du lien de causalité entre cet acte contraire et le dommage subi par elle. Ainsi, la reprise d'un renseignement sur l'origine ethnique d'un demandeur de crédit, donnée assurément non pertinente et interdite suivant l'article 6, peut ne pas être la cause du refus de crédit opposé au demandeur.

5. — LES TRANSFERTS DE DONNÉES VERS DES PAYS TIERS

66. — L'article 21 de la nouvelle loi remplace la disposition ancienne selon laquelle le Roi pouvait régler ou interdire « les rapprochements, interconnexions des traitements, ou toute autre forme de mise en relation de données à caractère personnel », disposition devenue sans objet, énonce l'exposé des motifs, eu égard « à la situation actuelle de la technologie de l'information » (175).

Le premier alinéa reprend le principe énoncé par l'article 25 de la directive : un transfert de données vers un pays tiers n'est autorisé que si le pays assure un niveau de protection adéquat et, ajoute la loi, moyennant le respect des autres dispositions de la présente loi et de ses arrêtés d'exécution (176).

L'article 21 précise en son alinéa 2 les critères d'appréciation du caractère adéquat. Il paraphrase la directive lorsqu'il dispose que : « Le caractère adéquat du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données. Il est notamment tenu compte de la nature finale, des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées ».

(175) Exposé des motifs, p. 58. L'avis de la Commission approuve cette réflexion (Avis, p. 23, n° 50). Que veut-on dire par là? La phrase prise en soi a une portée à ce point absolue qu'on pourrait en déduire que toute réglementation est devenue inutile dans la mesure où la technologie permettrait de la contourner, ce qui est pour le moins contestable.

(176) La signification de cet ajout est peu évidente. S'agit-il de rappeler que le transfert constitue pour l'exportateur un traitement qui doit lui-même répondre aux conditions de licéité fixées par la loi et ses arrêtés d'exécution? Ainsi, le transfert correspond-il dans le chef de l'exportateur à une finalité légitime, son contenu est-il proportionné à la finalité ainsi invoquée, les personnes concernées ont-elles été informées, etc.?

67. — L'appréciation du caractère adéquat revient, dit la Commission belge (177), au responsable du traitement localisé en Belgique. L'assertion est maladroite. On peut certes estimer qu'un régime d'autorisation au cas par cas ou par catégorie de flux apparaît inutilement administratif et lourd. On conçoit à l'inverse difficilement que le responsable se trouve livré à lui-même pour déterminer si oui ou non le flux qu'il envisage respecte le requis de la loi. Le groupe dit de l'article 29 de la directive (178) a établi une méthodologie d'analyse des flux et fixé les critères du caractère adéquat de la protection (179). Il serait aberrant que ce texte européen n'ait aucune portée obligatoire et que son respect par les responsables de traitements ne fasse l'objet d'aucun contrôle. Or, aucune référence n'est faite ici au pouvoir du Roi de fixer les critères du caractère adéquat.

Par contre, il est loisible pour le Roi, « après avis de la Commission de protection de la vie privée et conformément à l'article 25 de la directive 95/46/C.E.E. ... » de déterminer « pour quelles catégories de traitements et dans quelles circonstances, la transmission n'est pas autorisée ». Cette solution de la « liste noire » a été substituée en dernière minute à celle de la « liste blanche » (180), solution qui, à la suite de l'avis de la Commission (181), avait été jugée comme trop limitative des flux puisqu'elle aurait conduit à n'admettre d'exportation de données que vers les pays relevant de cette liste. A l'inverse, cette solution de la « liste noire » est illusoire dans la mesure où on sait que la décision d'inscrire un pays dans la liste noire est bien trop délicate politiquement. Bref, l'utilisation par le Roi des prérogatives qui lui sont confiées par l'article 21, § 2 risque d'être exceptionnelle et

(177) Avis, n° 54.

(178) Document de travail adopté par le groupe le 24 juillet 1998 : « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données ». Ce document est accessible et peut être téléchargé à l'adresse http://europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm. Le lecteur trouvera du reste sur ce site, d'autres documents et études relatives à la directive. Ce document reprend les conclusions de l'étude : Y. Poullet et B. Havelange, *Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel*, janv. 1997, Annexe au rapport annuel 1998 (XV D/5047/98) du groupe de travail établi par l'article 29 de la directive 95/46/C.E., Office des publications européennes, ISBN 92-828-4305-X.

(179) Le document analyse également l'interprétation à donner aux exceptions prévues par l'article 26 de la directive.

(180) La directive prévoit à la fois la possibilité de liste noire (art. 25.4) et de liste blanche (art. 25.6). Sur ces listes et les procédures mises en place par la directive pour les établir, voy. La protection des données à caractère personnel en droit communautaire, p. 174.

(181) Avis, n° 54.

n'être jamais que le suivi d'une décision européenne.

68. — L'article 22 de la directive retranscrit littéralement (182) les deux exceptions à l'exigence d'une protection adéquate énoncées par l'article 26 de la directive. L'article 22, § 1er vise des cas particuliers qui tiennent compte du contexte dans lequel s'inscrit le flux (consentement de la personne concernée, nécessité de l'exécution d'un contrat, etc.). Ces exceptions doivent être interprétées restrictivement (183).

Le paragraphe 2 du même article exige qu'à défaut de protection adéquate offerte par le pays tiers, celle-ci soit offerte par le mécanisme de « garanties suffisantes », notamment contractuelles. Ainsi, si une entreprise multinationale désire transférer les données relatives à son personnel, sans consentement de celui-ci, dans un pays n'offrant pas de protection adéquate, il lui revient par des mécanismes variés tantôt de sécurité technique, tantôt organisationnels (nomination d'un détaché chargé de veiller au respect dans le pays du destinataire des normes de protection des données), tantôt enfin par des clauses contractuelles à objet varié (reconnaissance d'un droit d'accès et de rectification, limitation des finalités d'utilisation, ...), de procurer des « garanties suffisantes » quant au respect effectif des principes de la protection des données.

Le Roi doit autoriser de tels transferts. L'autorisation sera-t-elle au cas par cas ou par catégories de flux? L'autorisation sera-t-elle donnée sur avis de la Commission ou sur simple notification à celle-ci? On rappellera à cet égard que selon l'article 26, § 3, de la directive, la Commission européenne a exigé d'être informée des autorisations et que celles-ci peuvent être l'objet d'opposition de la Commission elle-même et des autres Etats membres. Le souci que ce paragraphe exprime est de ne pas créer de distorsions de concurrence (184) par le biais de politiques d'autorisations soit trop laxistes, soit trop sévères. Il explique également la possibilité prévue par le même article pour la Commission d'arrêter des clauses contractuelles types satisfaisant aux critères de « garanties suffisantes ».

6 CONCLUSIONS

69. — Sans doute, est-il malaisé sans recul, sans connaissance du contenu des arrêtés royaux qui compléteront l'arsenal réglementaire belge, de tirer dès maintenant des conclusions sur les modifications de la loi du 8 décembre 1992.

L'absence de débats au sein et autour de l'enceinte parlementaire explique sans doute que les rédacteurs de la loi n'aient pas toujours pris la juste mesure des équilibres mis en place par la directive et n'aient pas su profiter des solutions innovantes proposées par cette dernière — en particulier, celle du préposé à la protection des données. On regrette également que le législateur n'ait pas tenté de tirer les leçons de six années d'application de la loi (185).

La pratique avait montré à quel point l'ancien texte était difficile à appliquer car peu compréhensible pour tout un chacun. Nombre de responsables du traitement s'étaient quelque peu découragés et désintéressés de la matière. Profitant de l'absence presque totale de contrôle effectif de l'application de la loi, ils se sont souvent contentés d'une mise en application de façade. De ce point de vue, la situation risque d'empirer avec la nouvelle loi.

70. — En ce qui concerne les entreprises, le bilan est contrasté. On tend à leur reconnaître une plus grande facilité de traitement de l'information — y compris sensible — par l'entrée en force du consentement de la personne concernée comme élément de légitimation du traitement et l'allégement des formalités de déclaration. L'expérience montre cependant que l'obtention du consentement est souvent difficile — sauf peut-être au moyen des nouvelles techniques comme sur l'Internet — car réclamant une démarche positive de la personne concernée, elle est malaisée à mettre en œuvre. L'allégement de l'obligation de déclaration risque en outre d'être compensée par le renforcement de l'obligation d'information.

Certaines administrations voient leur vie facilitée, ainsi les administrations de la sécurité de l'Etat et de la sécurité sociale. Pour ce faire, des exceptions ont été utilisées de manière extensive et des notions ont été étendues au-delà du champ d'application qu'entendait leur réserver la directive. On peut donc craindre qu'une loi à deux vitesses ne se profile au bénéfice du secteur public et au détriment de la personne concernée par les données.

Et l'autorité de contrôle dans tout cela? La directive donnait au législateur belge la possibilité d'élargir ses compétences et par là d'en repenser le statut, le fonctionnement et la composition : rien n'a été fait en la matière. En l'absence de toute politique de poursuite pénale des infractions à la loi, le manque d'effectivité et d'efficacité du contrôle non judiciaire risque de peser lourd pour l'avenir de la protection. Ici aussi, des leçons auraient pu être tirées de l'expérience acquise au cours de ces dernières années. La protection judiciaire est, en la matière, un leurre. Les personnes concernées — et qui peut leur en faire le reproche? — ne sont pas prêtes à en supporter le coût. Sauf avantage patrimonial à la clé — la conclusion d'un contrat de crédit ou d'assurance par exemple — elles ne perçoivent pas bien les dangers issus du non-respect de la loi. L'intérêt de la personne concernée — qui porte uniquement sur ses propres données — est en outre assez faible par rapport à l'intérêt du responsable du traitement pour lequel la valeur du traitement se mesure sur l'ensemble des données à caractère personnel dont il dis-

(182) L'article 26 de la directive autorisait cependant le droit national à émettre des réserves vis-à-vis des exceptions prévues par cet article.

(183) A ce propos, voy. La protection des données à caractère personnel en droit communautaire, p. 174.

(184) Sur ce souci, lire en particulier le document de travail du groupe de l'article 29, déjà cité, qui affirme notamment : « Compte tenu de la complexité et de la difficulté manifestes de ces solutions contractuelles, il est, de toute évidence, nécessaire, de fournir aux responsables du traitement qui envisagent de recourir à des contrats dans cette entreprise des orientations arrêtées en commun. Au niveau des Etats membres, il est probable qu'il appartiendra essentiellement aux autorités nationales compétentes de fournir ces orientations, en particulier lorsqu'elles prépareront les autorisations prévues à l'article 26, § 2. Les autorités nationales et la Commission devraient coopérer et se consulter, sur les clauses contractuelles qui leur seront présentées. Pour les cas où les clauses contractuelles types proposées seraient soumises soit aux autorités nationales, soit directement à la Commission, il conviendra de concevoir une procédure visant à garantir que ces clauses seront également examinées par le groupe de manière à éviter que des différences dans les pratiques nationales se fassent jour et à garantir que la Commission européenne sera en mesure de bénéficier des conseils avisés d'experts avant de prendre une décision en application de l'article 26, § 4 ».

(185) Une évaluation systématique de l'application de la loi ancienne en pratique a été suggérée par le Conseil d'Etat mais refusée par le ministre, prétextant un manque de recul dû au bref laps de temps écoulé entre l'entrée en vigueur des dernières dispositions de la loi du 8 décembre 1992 et le moment où le Conseil d'Etat a rendu son avis (Rapport, p. 8). Cette raison ne convainc pas. La plupart des dispositions de la loi étaient en vigueur avant juin 1996. Le travail accompli depuis 1994 par la Commission de la protection de la vie privée aurait pu servir de base à la réflexion. Il est à noter que plusieurs pays voisins ont préféré prendre du retard dans la proposition afin d'évaluer les acquis des années d'application de ce type de législations (France, Pays-Bas).

pose. La réaction privilégiée devrait donc provenir de la société elle-même représentée par les différents organes de contrôle ayant le pouvoir d'intervenir.

71. — Ces quelques constatations ne poussent pas réellement à l'optimisme. Sans doute doit-on y voir un manque criant de volonté politique quant à la mise en place effective d'une protection pourtant de plus en plus nécessaire dans une société belge de l'information qui se dessine de manière pour le moins confuse. Le salut pourrait peut-être provenir des organisations internationales qui, comme la Commission européenne et les organes de réflexion et de contrôle qui fonctionnent en son sein, ont le pouvoir d'imposer à la Belgique un certain « dynamisme » en la matière.

Thierry LÉONARD
Yves POULLET

TABLE DES MATIÈRES

Introduction

1999 **1. Les définitions et le champ d'application de la loi**

396

1.1. Les définitions modifiées
1.2. Le champ d'application matériel et personnel
1.2.1. Les exceptions au bénéfice des traitements à finalité journalistique ou d'expression littéraire ou artistique
1.2.2. Les autres exceptions au champ d'application matériel
1.3. Le champ d'application territorial

2. Les lignes directrices de la protection

2.1. Le principe de finalité des traitements
2.1.1. Le principe de légitimité des traitements
2.1.2. Les principes de conformité et de qualité des données
2.2. Le traitement des données « sensibles »
2.2.1. Les données « sensibles » au sens strict
2.2.2. Les données relatives à la santé
2.2.3. Les données « judiciaires »
2.2. Le traitement des données « sensibles »

3. Les droits de la personne concernée

3.1. Le droit à l'information
3.2. Les droits d'accès et d'opposition
3.3. La non-soumission à des décisions individuelles automatisées

4. Le contrôle des traitements

4.1. Le contrôle interne
4.2. Le contrôle externe
4.2.1. Le contrôle spécialisé : la Commission de protection de la vie privée
4.2.1.1. L'instrument de contrôle : la déclaration
4.2.1.2. Les compétences de la Commission
4.2.1.3. La composition de la Commission
4.2.2. Les autorités administratives et juridictionnelles

5. Les transferts de données vers des pays tiers

Conclusions