

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La nouvelle loi belge de protection des données à caractère personnel

de Terwangne , Cécile

Published in:

La protection de la vie privée dans la société d'information

Publication date:

2002

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

de Terwangne , C 2002, La nouvelle loi belge de protection des données à caractère personnel. dans *La protection de la vie privée dans la société d'information*. Cahier des sciences morales et politiques, Presses universitaires de France, Paris, pp. 91-109.

General rights

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

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

Take down policy

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

Cécile de Terwangne
Docteur en Droit
Directrice de recherches
au Centre de Recherches Informatique et Droit

Introduction

Il y a tout juste trente ans, la Belgique était un des premiers Etats du monde à voir une proposition de loi déposée au Parlement, visant à protéger la vie privée des citoyens face à l'informatique. De nombreuses années devaient toutefois jalonner le parcours législatif d'une telle préoccupation. Et de pionnière, la Belgique est bientôt passée à l'état de retardataire dans le concert des nations européennes.

En effet, le 21 janvier 1981, le Conseil de l'Europe adoptait la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Dès 1982, la Belgique signait cette convention. Ce faisant, elle s'engageait à l'égard des Etats cosignataires à adopter une législation interne réglementant l'utilisation des données personnelles.

Ce n'est qu'à la fin de 1992 que la Belgique s'est dotée d'une loi en la matière. Destinée en quelque sorte à apurer une dette du passé, cette loi du 8 décembre 1992¹ aurait pu être porteuse de dividendes pour l'avenir puisque l'on pressentait à l'époque l'adoption imminente d'une directive européenne sur le sujet. Le législateur belge aurait pu anticiper les obligations qui ne manqueraient pas de lui être imposées par le législateur européen. Il a toutefois fallu se rendre à l'évidence : les anticipations, s'il y en eut, n'ont pas vraiment permis à la Belgique d'échapper, une fois la directive adoptée, à un exercice de mise à jour suffisamment important pour que l'on évoque une véritable révolution de la loi.²

La directive 95/46/CE du 24 octobre 1995³ accordait 3 ans aux Etats membres pour mettre leur législation en conformité avec ses prescrits. La Belgique n'eut en apparence que quelques semaines de retard sur ce délai puisque c'est le 11 décembre 1998 qu'elle votait la loi modifiant la loi du 8 décembre 1992⁴. Cette loi n'est en fait entrée en vigueur que le 1^{er} septembre 2001. En outre, pour de nombreuses dispositions un arrêté d'exécution était nécessaire. Cet arrêté a été adopté le 13 février 2001⁵ mais n'est également entré en vigueur

¹ Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Moniteur belge (M.B.)*, 18 mars 1993.

² TH. LEONARD et Y. POULLET, « 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 », *J.T.*, 1999, pp. 377 et s.

³ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 23 novembre 1995, n° L 281, p. 31. Sur la directive, voy. M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, pp. 121 et s.

⁴ Loi du 11 décembre 1998 transposant la directive 95/46/CE 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 février 1999.

⁵ Arrêté royal du 13 février 2001 portant exécution 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.* 13 mars 2001

que le 1^{er} septembre 2001. La quasi ponctualité de la Belgique au regard des attentes européennes n'était donc que relative.

A l'instar de la Convention 108 et de la directive 95/46, la loi belge vise explicitement à protéger les libertés et droits fondamentaux des personnes physiques, et notamment leur vie privée. La vie privée, dans ce contexte, ne doit pas se comprendre comme un ensemble d'informations personnelles que l'on souhaite garder cachées. Elle est à entendre comme autodétermination informationnelle, c'est-à-dire comme autonomie dans la détermination des conditions de communication de données à caractère personnel⁶. La vie privée c'est la maîtrise par chacun de son image informationnelle.

Les pages qui suivent seront consacrées à une description de la situation législative belge nouvelle. Elles porteront sur l'analyse du champ d'application de la loi belge dans sa nouvelle version (section 1^{re}), sur la question de la licéité des traitements de données ordinaires et des traitements de données sensibles (section 2.), sur les devoirs et droits liés au principe de transparence ainsi que sur les nouveaux droits reconnus aux personnes concernées par les données (section 3.) et sur les différentes formes de contrôle établies par la loi (section 4.).

Section 1.

Champ d'application de la législation relative à la protection des données à caractère personnel

A. La notion de « donnée à caractère personnel »

La loi belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel donne de la « donnée à caractère personnel » une définition textuellement reprise de la directive européenne en la matière. Par cette expression on entend « toute information concernant une personne physique identifiée ou identifiable », sachant qu'est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale⁷.

Plutôt qu'opter pour une évaluation *in concreto* du caractère identifiable, c'est-à-dire en tenant compte des moyens à disposition du responsable du traitement des données, l'Exposé des motifs de la loi signale qu'il convient d'évaluer *in abstracto* le caractère identifiable. Désormais, pour déterminer si une personne est identifiable, il faut prendre en compte « l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement *ou par toute autre personne*, pour identifier les sujets de données ». Si celui qui utilise les données n'a pas lui-même la possibilité d'identifier les individus

⁶ Voy. H. BURKERT, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'Informatique et des Télécoms*, 1985, 8-16 ; C. DE TERWANGNE, « Le rapport de la vie privée à l'information », in *Droit des technologies de l'information. Regards prospectifs* (sous la direction d'E. MONTERO), Cahier du CRID n° 16, Bruxelles, Bruylant, 1999, p. 144 ; Th. LEONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », in F. RIGAUX, *La vie privée : une liberté parmi les autres ?*, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.

⁷ Art. 1er, § 1er nouveau de la loi belge du 8 décembre 1992.

correspondant aux données mais qu'il se trouve quelqu'un apte à le faire, les données doivent tout de même être considérées comme étant « à caractère personnel ». Et la loi s'appliquera.

Bref, dès lors qu'elle porte sur un individu identifié ou identifiable, toute information est qualifiée de « donnée à caractère personnel » au sens de la législation relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Il peut s'agir d'un numéro de plaque de voiture, de données contenues dans un répertoire d'adresses, professionnel ou non, de photos, de données invisibles transmises lors de sessions Internet (adresses IP permanentes), de données bibliographiques, de l'identification des parties, des juges et des plaideurs dans les décisions de jurisprudence, etc.

B. Le traitement des données à caractère personnel

Pour que s'applique la législation de protection des données à caractère personnel, il faut être en présence d'un traitement de telles données. Les règles protectrices s'appliquent en effet à toute opération ou ensemble d'opérations effectuées en tout ou en partie 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 personnel⁸.

Le champ d'application matériel de la loi est élargi par rapport au régime antérieur. Les opérations couvertes sont particulièrement variées et vont, cette fois, de la collecte à la consultation d'informations à caractère personnel, jusqu'à la communication par transmission, diffusion ou toute autre forme de mise à disposition de ces informations. Ces opérations correspondent en tout cas à un traitement de données si elles impliquent, ne fût-ce qu'en partie, le recours à des moyens automatisés. Il suffit, par exemple, que les informations soient au départ conservées sur un support informatisé et ensuite imprimées, ou qu'elles soient transmises en faisant usage de procédés automatisés, même si elles sont sur support papier (fax). Les moyens automatisés englobent toutes les technologies de l'information : informatique, télématique, réseaux de télécommunication.

La loi s'applique également si les opérations se font sans le moindre recours à des procédés automatisés, pourvu que les données sur lesquelles portent la ou les opérations soient contenues ou appelées à figurer dans un fichier⁹. Par fichier, il faut entendre un « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »¹⁰. La notion de fichier se distingue de celle de « dossier ». La loi exclut les dossiers non structurés de son champ. Le critère de distinction entre fichier et dossier se situe dans le degré d'accessibilité des données contenues. Ces données doivent être

⁸ Art. 1er, § 2 et art. 3, § 1er nouveaux de la loi du 8 décembre 1992. Sur le fait qu'une seule opération suffit pour qu'il y ait traitement et les difficultés qui en découlent, voy. M.-H. BOULANGER et C. DE TERWANGNE, "Internet et le respect de la vie privée", in *Internet face au droit*, Cahier du CRID n° 12, Bruxelles, Story-Scientia, 1997, p. 198.

⁹ Art. 3, § 1er nouveau de la loi du 8 décembre 1992.

¹⁰ Art. 1er, § 3 nouveau de la loi du 8 décembre 1992.

accessibles selon des critères déterminés pour que l'ensemble soit considéré comme fichier (par exemple un classement sur la base des noms des personnes, par ordre alphabétique).¹¹

En résumé, lorsqu'aucun procédé automatisé n'intervient dans les opérations effectuées sur les informations, la législation de protection des données à caractère personnel ne s'appliquera pas si les informations proviennent de dossiers, ou de documents non classés dans un fichier. La consultation de documents papier isolés ou l'envoi par courrier ordinaire de photocopies de documents papier qui ne sont pas extraits d'un « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés », peuvent se faire, par exemple, sans tenir compte des principes régissant la protection des données à caractère personnel.

Il est à noter que les dispositions contenues dans la législation de protection des données à caractère personnel s'appliquent tant au secteur public qu'au secteur privé. Il est donc indifférent, pour la prise en compte des principes de protection des données, que le détenteur des informations soit une entité publique ou privée.

C. Le responsable du traitement

La notion de « responsable du traitement » désigne 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 personnel¹². Dans l'exposé des motifs du projet de la future loi relative à la protection des données à caractère personnel du 11 décembre 1998, adaptant la loi belge de 1992 à la directive européenne en la matière, le ministre a précisé que c'est la personne investie du pouvoir de décision sur le traitement de données qui est visée par la notion de responsable du traitement¹³.

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 ou morale, l'association de fait ou l'administration publique désignée comme tel par le texte en question¹⁴.

¹¹ La différence entre fichier et dossier a déjà fait couler beaucoup d'encre et a fait l'objet en Belgique d'un arrêt en cassation : Cass., 16 mai 1997, *J.T.*, 1997, p. 779 ; Anvers, 27 septembre 1995, *A.J.T.*, 1995-96, note J. DUMORTIER ; TH. LEONARD, « La protection des données à caractère personnel et l'entreprise », in *Guide juridique de l'entreprise*, 2ème éd., Titre XI, Livre 112, Diegem, Kluwer, 1996, p. 15, n° 130 ; en France, voy. notamment : Cass. (ch. crim.), 3 novembre 1987, *D.*, 1988, J, pp. 17 et s., note H. MAISL ; T.G.I. Créteil, 10 juillet 1987, *D.*, 1988, J., pp. 319 et s., note J. FRAYSSINET ; J. FRAYSSINET, « La Cour de Cassation et la loi informatique, fichiers et libertés ou comment amputer une loi tout en raffermissant son application », *J.C.P.*, 1988, I, n° 3223 ; IDEM, « Contre l'excessive distinction entre fichier et dossier – Le pas en avant du tribunal correctionnel de Paris », *Expertises*, 1990, pp. 16 et s.

¹² Art. 1er, § 4 nouveau de la loi du 8 décembre 1992. Sur la préférence à accorder au seul critère du pouvoir de détermination des finalités, voy. M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, « 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.

¹³ Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement 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, Exposé des motifs, *Doc. Parl.*, Ch. Repr., sess. ord. 1997-1998, n° 1566/1, p. 15.

¹⁴ Art. 1er, § 4, al. 2 nouveau de la loi du 8 décembre 1992.

D. Les exceptions

Des exceptions sont prévues, soit globales, soustrayant certains traitements de données à l'ensemble de la loi, soit partielles, dispensant du respect de certaines dispositions de la loi. Bénéficient de l'exception globale les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques¹⁵.

Les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire entrent, eux, dans la catégorie d'exceptions partielles. Une série de dispositions peuvent ne pas être appliquées à ces traitements, afin de garantir un équilibre avec la protection de la liberté d'expression¹⁶.

D'autres exceptions partielles, pour classiques qu'elles soient, sont particulièrement larges. Il s'agit des exceptions accordées aux traitements effectués à des fins de sécurité publique¹⁷. Il est étonnant et particulièrement dommage que ces exceptions n'aient fait l'objet d'aucun débat au sein de la société, ou à tout le moins au sein du Parlement, au moment de leur adoption. Ni le Conseil d'Etat, ni même la Commission de la protection de la vie privée ne se sont insurgés contre l'ampleur de ces exceptions dans les avis qu'ils ont rendus sur le texte qui leur était soumis à l'état de projet. Ceci est d'autant plus regrettable que « 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 »¹⁸.

E. Le champ d'application territorial de la loi

Le législateur belge, suivant la directive, a modifié le critère de rattachement déterminant l'applicabilité de la loi. Il s'est définitivement écarté de la notion de « fichier », déterminante dans les premières générations de législations en la matière et basée sur une localisation physique précise des données (sur une disquette, sur le disque dur d'un ordinateur identifié,...). Il n'a plus retenu non plus la localisation du traitement, celui-ci pouvant désormais être effectué sur des données qui ne sont pas rassemblées dans un « lieu » unique. C'est le lieu d'établissement fixe¹⁹ du responsable du traitement qui est à présent le critère d'applicabilité de la loi²⁰. Si le responsable d'un traitement a un établissement fixe sur le territoire belge, c'est la loi belge qui s'appliquera au traitement effectué par le responsable dans le cadre des activités réelles et effectives de cet établissement. Ainsi, si un complexe hôtelier localisé en Belgique offre un service de réservation via Internet et demande en

¹⁵ Art. 3, § 2 nouveau de la loi du 8 décembre 1992.

¹⁶ Art. 3, § 3 nouveau de la loi du 8 décembre 1992.

¹⁷ Art. 3, §§ 4 et 5 nouveau de la loi du 8 décembre 1992.

¹⁸ Y. POULLET et B. HAVELANGE, « Secrets d'Etat et vie privée ou comment concilier l'inconciliable ? », in *Droit des Technologies de l'information Regards prospectifs*, Cahier du CRID n° 16, Bruxelles, Bruylant, 1999, n° 15.

¹⁹ Le considérant 19 de la directive 95/46/CE précise que « l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. [...] 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 ce sujet ».

²⁰ Art. 3bis, al. 1^{er}, 1^o nouveau de la loi du 8 décembre 1992.

conséquence aux intéressés d'enregistrer leurs coordonnées afin d'effectuer la réservation, la loi belge de protection des données trouvera à s'appliquer au traitement de ces informations.

A l'instar du législateur européen, le législateur belge s'est préoccupé des tentatives de contournement du régime de protection mis en place, par la délocalisation de l'établissement du responsable du traitement. Afin d'éviter pareille situation, le texte²¹ prévoit que tout responsable qui n'est pas établi de manière permanente sur le territoire de la Communauté européenne mais qui recourt à des moyens, automatisés ou non, situés sur le territoire belge, dans le but de traiter des données personnelles, est soumis à la loi du 8 décembre 1992 modifiée. Il est tenu en outre de désigner un représentant établi sur le territoire belge²². Le seul transit de données sur le territoire belge n'est toutefois pas couvert par la loi.

Dans le monde en réseau que nous connaissons, et principalement dans le contexte d'Internet, une telle solution est excessive et impraticable. Elle conduit en effet à étendre l'application de la loi belge à tout utilisateur d'Internet qui copie ou télécharge des informations nominatives à partir d'un site Web ouvert par un fournisseur d'informations établi en Belgique²³. Ce faisant, l'internaute effectue en effet un traitement de données en recourant à des moyens automatisés²⁴ situés en Belgique. Il est donc tenu de respecter la loi belge et de désigner un représentant établi dans notre pays. Il en va de même pour tout responsable de site Web de par le monde qui invite les internautes, via le site, à communiquer des informations nominatives. Lorsqu'un internaute communique ses données par des moyens situés sur le territoire belge (son ordinateur, les installations de son fournisseur d'accès, les appareils de télécommunications), la collecte réalisée par le responsable du site est désormais soumise à la loi belge et le responsable doit désigner un représentant en Belgique. C'est assurément irréaliste.

Pour garder à l'article 3*bis* une portée effective, la seule lecture de cette disposition qui, à notre sens, s'impose, est une lecture téléologique. La *ratio legis* de cet article se résume clairement dans la volonté d'éviter que les individus se retrouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation²⁵. Le souci des auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la loi, même en dehors des frontières.

C'est par une lecture combinée de l'article 3*bis* et des articles 21 et 22 qui régissent les flux transfrontières vers les Etats non membres de la Communauté européenne qu'une définition rationnelle de l'applicabilité de la loi pourra être dégagée.

On peut en effet considérer qu'une première réponse à la préoccupation du législateur est donnée par l'instauration d'un régime protecteur en matière de flux transfrontières de

²¹ Art. 3*bis*, al. 1^{er}, 2^o nouveau de la loi du 8 décembre 1992.

²² Art. 3*bis*, al. 2 nouveau de la loi du 8 décembre 1992.

²³ Sur le raisonnement attaché à cet exemple, voy. M.-H. BOULANGER et C. DE TERWANGNE, *op. cit.*, pp. 201-202.

²⁴ L'exposé des motifs de la loi du 11 décembre 1998 signale que "le terme "moyens" recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunications, 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." (*Doc. parl.*, Ch. repr., sess. ord. 1997-98, n° 1566/1, p. 27).

²⁵ Voy. l'exposé des motifs (*Doc. parl.*, Ch. repr., sess. ord. 1997-98, n° 1566/1, p. 27) et le considérant 20 de la directive.

données en dehors de la Communauté européenne. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi s'imposent à tous les acteurs qui effectuent des opérations sur des données transférées à partir de la Belgique. Une protection adéquate des données envoyées à l'étranger en provenance de Belgique est exigée.

La réponse contenue à l'article 3*bis* vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manœuvre artificielle, du bénéfice de la protection de l'ensemble de la loi, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontières. Dans ce sens, deux catégories de situations entrent selon nous, dans le champ de l'article 3*bis* :

- celle précisément où un responsable de traitement de traitement cherche délibérément à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés sur le territoire belge pour réaliser son traitement ;
- celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. C'est le cas d'une collecte de données effectuée par le biais de *cookies*, à l'insu de la personne concernée, au sein même de son ordinateur. Les *cookies* auront été discrètement déposés par le responsable d'un site Internet sur le disque dur du « surfeur » belge, à l'occasion d'une de ses visites du site en question. Les dispositions concernant les flux transfrontières de données ne trouvent pas à s'appliquer à cette hypothèse²⁶. Pour combler le vide de protection, l'article 3*bis* a alors toute sa pertinence. C'est donc le régime complet de la directive qui va s'appliquer au traitement de données obtenues à l'aide de *cookies*, et non le régime spécifique –plus souple– des flux transfrontières.

Dans ces deux hypothèses, le critère déterminant de l'application de la loi belge aux responsables établis hors de la Communauté européenne ne se réduit pas à l'utilisation de moyens situés sur le territoire du pays. Cette utilisation n'est qu'un élément de l'analyse du contexte des opérations effectuées. Une analyse plus globale s'impose en effet pour pouvoir constater le cas échéant que le responsable du traitement est anormalement établi à l'étranger alors que son activité est orientée sur la Belgique, ou que l'on se trouve en présence d'une situation échappant à toute protection, notamment à celle issue du régime des flux transfrontières.

Section 2.

Licéité des traitements de données à caractère personnel

La directive européenne 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 prévoit les conditions auxquelles un traitement des données doit répondre pour être admissible²⁷. Ces conditions ont été reproduites dans la loi belge²⁸.

A. Respect du principe de finalité

²⁶ Voy. l'explication détaillée donnée dans M.-H. BOULANGER et C. DE TERWANGNE, *op. cit.*, p. 203.

²⁷ Art. 6 et 7 de la directive du 24 octobre 1995.

²⁸ Art. 4 et 5 nouveaux de la loi du 8 décembre 1992.

Pour être licite, un traitement de données à caractère personnel doit poursuivre une finalité déterminée, explicite et légitime²⁹ et s'identifier à une des hypothèses reprises dans la liste de l'article 5 de la loi de 1992.

Déterminée(s) et explicite(s), la ou les finalité(s) de la collecte des données ne peu(ven)t être secrète(s), camouflée(s).

Les finalités doivent en outre être légitimes. Bien que ce terme ne soit pas explicitement précisé dans la législation de protection des données, la doctrine s'accorde pour estimer que pour être légitime, la finalité ne peut induire une atteinte disproportionnée aux intérêts de la personne concernée par les données, au nom des intérêts poursuivis par le responsable du traitement³⁰. La notion de légitimité invite donc à une mise en balance des intérêts en présence.

Par ailleurs, l'article 5 nouveau de la loi du 8 décembre 1992³¹ énonce les six seules hypothèses dans lesquelles un traitement de données peut être effectué. Ces hypothèses représentent en fait les situations dans lesquelles l'équilibre des intérêts en présence est a priori atteint. M.-H. Boulanger, intervenant au nom de la Commission (belge) de la protection de la vie privée, signala lors des discussions qui accompagnèrent le vote de la modification de la loi belge, que les situations visées par l'article 5 de la loi créent « une présomption d'équilibre d'intérêts »³².

Les deux dispositions doivent être lues conjointement. Le fait de se trouver dans une des situations énoncées à l'article 5 n'implique pas que l'exigence de légitimité de l'article 4 soit *ipso facto* rencontrée. Les hypothèses visées dans la deuxième disposition n'empêchent pas un contrôle sur la base de la première. En fait, on peut considérer 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, sur la base de l'article 4, permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu³³.

Au titre des hypothèses autorisant le traitement de données, on trouve le consentement indubitable de la personne concernée³⁴, le cas du traitement « 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 »³⁵, du traitement « nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une

29 Art. 4, § 1e, 2° de la loi du 8 décembre 1992.

30 M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, *op. cit.*, pp. 377 et 379 ; Th. LEONARD, 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.*, 1993/4, pp. 1409 et s. ; J. DUMORTIER, F. ROBBEN, note sous Com. Anvers (Prés.), 7 juillet 1994 et Com. Bruxelles (Prés.), 15 septembre 1994, *Computerrecht*, 1994, pp. 244 et s.

31 Reproduction de l'article 7 de la directive du 24 octobre 1995.

32 In Rapport fait au nom de la Commission de la justice, *Doc. parl.*, ch. repr., sess. ord. 1998-1999, n° 1566/10, p. 47.

33 M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, *op. cit.*, p. 148, n° 41.

34 Art. 5, al. 1^{er}, *littera* a de la loi du 8 décembre 1992.

35 Art. 5, al. 1^{er}, *littera* b de la loi du 8 décembre 1992.

loi, d'un décret ou d'une ordonnance »³⁶, du traitement « nécessaire à la sauvegarde de l'intérêt vital de la personne concernée »³⁷, du traitement « 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 »³⁸ et enfin, du traitement « nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée »³⁹.

B. Traitements ultérieurs compatibles avec la finalité de collecte des données

Aux termes de l'article 4, § 1^{er}, 2^o de la loi belge de protection des données, les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [...] »⁴⁰.

1. Compatibilité ou incompatibilité

Dans certaines hypothèses, l'utilisation des informations à caractère personnel pourra être considérée comme compatible avec les finalités pour lesquelles ces informations ont été recueillies.

La loi belge précise que pour évaluer la compatibilité des utilisations des données survenant ultérieurement à la collecte, il faut tenir compte de tous les facteurs pertinents, et notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. En ce sens, on peut considérer que le critère de compatibilité est lié à l'un des principes majeurs de la législation de protection des données, à savoir la transparence des traitements de données à l'égard des personnes concernées par les données. Ce principe implique que la personne sur qui portent les données connaisse en toutes circonstances les utilisations qui sont faites des données. Le critère de compatibilité des traitements ultérieurs est donc logique lorsqu'il renvoie à la connaissance effective ou à l'attente raisonnable de la personne concernée^{41 42}.

36 Art. 5, al. 1^{er}, *littera* c de la loi du 8 décembre 1992.

37 Art. 5, al. 1^{er}, *littera* d de la loi du 8 décembre 1992.

38 Art. 5, al. 1^{er}, *littera* e de la loi du 8 décembre 1992.

39 Art. 5, al. 1^{er}, *littera* f de la loi du 8 décembre 1992.

40 Cette disposition est une reprise littérale de l'art. 6, § 1^{er}, *littera* b, première phrase, de la directive du 24 octobre 1995.

41 C'est ce critère qui avait été suggéré *in* C. DE TERWANGNE et S. LOUVEAUX, « Data Protection and Online Networks », *Computer Law and Security Report*, 1997, vol. 13, n° 4, p. 239 et *in* M.-H. BOULANGER, C. DE TERWANGNE, *op. cit.*, pp. 205-206.

42 Le recours aux dispositions légales et réglementaires pour évaluer la compatibilité d'utilisations ultérieures ne devrait pas renier ce lien avec le principe de transparence à l'égard de la personne concernée puisque l'Exposé des motifs de la loi spécifie 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 » (Projet de loi transposant la directive 95/46/CE 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, Exposé des motifs, *Doc. parl.*, Ch. repr.,

Dans d'autres cas, l'utilisation de données à caractère personnel ne pourra passer pour compatible avec les finalités poursuivies lors de la collecte de ces informations.

Une communication à des fins commerciales⁴³ des données à caractère personnel recueillies par l'administration ne pourra, par exemple, au vu des considérations émises sur le critère de compatibilité, être considérée comme compatible avec les finalités de collecte. On ne peut, en effet, faire entrer dans l'attente raisonnable des personnes communiquant des données à une personne publique dans le cadre d'un rapport réglé par la loi (communication légalement obligatoire ou effectuée pour bénéficier d'un service public), une réutilisation commerciale de ces données.

2. Conséquences pratiques de la distinction

Les conséquences du caractère compatible ou non d'un traitement ultérieur avec les finalités initiales de collecte des informations ne sont pas négligeables.

S'il est considéré comme compatible avec les finalités initiales, le traitement ultérieur ne devra pas lui-même passer le test de la légitimité imposé par l'article 4, § 1^{er}, 2^o. Ce sont les finalités initiales qui auront dû être jugées légitimes. Toute utilisation compatible avec ces finalités légitimes est admissible en soi. En outre, compatible avec les finalités de collecte, le traitement ne constitue pas un traitement indépendant. Il ne doit dès lors pas non plus répondre à l'une des hypothèses de licéité des traitements contenue dans l'article 5 nouveau de la loi du 8 décembre 1992. Chaque traitement en soi (indépendant) doit correspondre à une de ces hypothèses de licéité, tandis que les « traitements compatibles » ne sont pas concernés comme tels par cette exigence.

Par contre, les traitements qui ne sont pas compatibles avec les finalités de collecte ne peuvent être rattachés au traitement initial des données. Ils ne sont pas pour autant interdits mais doivent être envisagés comme des traitements séparés, indépendants. Ils doivent dès lors répondre eux-mêmes à toutes les exigences édictées par la loi pour admettre un traitement comme licite.

C. Qualité des données

Dans sa nouvelle version, la loi belge énonce de façon plus détaillée qu'auparavant des exigences quant à la qualité des données faisant l'objet d'un traitement.

Une finalité déterminée et légitime n'autorise pas à traiter n'importe quelle donnée. Aux termes de l'article 4, § 1^{er}, 3^o, les données doivent être adéquates, pertinentes et non

sess. ord. 1997-1998, n° 1566/1). Le système belge n'opte pas, semble-t-il, pour une compatibilité automatique découlant de la seule existence de dispositions légales ou réglementaires. C'est particulièrement souhaitable étant donné que l'obligation d'information des personnes concernées, existant par ailleurs et pesant normalement sur tout responsable d'un traitement de données, n'existe pas pour les traitements prévus par la loi. Voy. également J. DUMORTIER, « Some legal issues related to the implementation of the European data protection Directive in the Belgian legal system », contribution présentée à la 19^{ème} Conférence internationale des Commissaires à la Protection des Données, Bruxelles, 17-19 septembre 1997, p. 6.

43 Les finalités commerciales sont envisagées ici tant dans le chef du secteur public : c'est l'administration qui souhaite vendre ses données, que dans le chef d'un tiers privé : c'est l'entreprise qui acquiert les données pour les intégrer dans un produit informationnel qu'elle veut commercialiser.

excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

Elles doivent être exactes et, si nécessaires, mises à jour. La loi précise qu'il incombe au responsable du traitement de prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités poursuivies, soient effacées ou rectifiées. C'est donc une obligation de moyen et non de résultat qui est mise à charge du responsable.

Enfin, les données ne peuvent être conservées que pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été obtenues ou pour lesquelles elles sont traitées ultérieurement. Elles peuvent toutefois être conservées au delà de cette période à des fins historiques, statistiques ou scientifiques, pourvu que le responsable respecte les conditions établies dans l'arrêté royal du 13 février 2001 à propos des traitements à de telles fins.⁴⁴

D. Régime des données sensibles, médicales et « judiciaires »

1. Principe

Le traitement des données visées aux articles 6 à 8 de la loi est en principe interdit. Il s'agit tout d'abord des données dites « sensibles », définies à l'article 6 comme étant les données à caractère personnel 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 sexuelle⁴⁵. L'article 7 vise, lui, les données à caractère personnel relatives à la santé. L'article 8 de la loi évoque les données « judiciaires », définies comme les 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 ». Cette dernière définition est étonnamment plus large que la définition présente dans la directive.

2. Exceptions

La loi prévoit des cas dans lesquels le traitement des données tant sensibles que médicales et judiciaires est admis, mais elle invite le Roi à fixer les conditions particulières auxquelles doit alors satisfaire le traitement des données.

Les données sensibles et les données relatives à la santé peuvent être traitées avec le consentement écrit de la personne concernée. Cette exception n'est toutefois plus valable lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement l'empêchant de refuser librement son consentement. Dans une telle situation, le consentement écrit est tout de même admis comme justifiant le traitement si celui-ci vise à octroyer un avantage à la personne concernée⁴⁶.

⁴⁴ Voy. chap. II de l'arrêté royal du 13 février 2001, précité.

⁴⁵ Y. POULLET, TH. LEONARD, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, p. 386.

⁴⁶ Art. 27 de l'arrêté royal du 13 février 2001.

Les données sensibles et les données relatives à la santé peuvent en outre être traitées si cela est nécessaire au vu des obligations et des droits du responsable du traitement en matière de droit du travail ; si c'est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'un tiers alors que la personne concernée est dans l'impossibilité de donner son consentement ; si le traitement porte sur des données manifestement rendues publiques par la personne concernée ; si le traitement est nécessaire à la défense d'un droit en justice ; s'il est nécessaire à des recherches scientifiques ; s'il est nécessaire en vue de l'application de la sécurité sociale ; s'il est nécessaire à des fins médicales ; s'il est rendu obligatoire par une norme législative pour un motif important d'intérêt public.

Les données sensibles peuvent en outre être traitées dans le cadre des activités de tout organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale pourvu que le traitement se rapporte aux seuls membres ou aux personnes entretenant des contacts réguliers avec cet organisme et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Les données médicales, quant à elles, peuvent être également traitées lorsque cela est nécessaire à la promotion et à la protection de la santé publique (dépistage,...).

Les données « judiciaires » peuvent être traitées si cela est nécessaire à l'exercice des tâches d'une autorité publique ou d'un officier ministériel ; si c'est nécessaire à la réalisation de finalités fixées par ou en vertu de la loi ; pour la gestion de contentieux ; pour la défense de clients par les avocats ou d'autres conseil juridiques ; pour les nécessités de la recherche scientifique.

Pour toutes ces hypothèses, des garanties supplémentaires, fixées par le Roi sont à observer :

- Selon l'article 25 de l'arrêté royal, le responsable du traitement doit désigner les catégories de personnes ayant accès aux données et décrire de manière précise leur fonction par rapport au traitement des données. Cela n'oblige pas le responsable du traitement à désigner les personnes par leur nom mais plutôt à établir des profils d'accès. Cette liste doit être tenue à la disposition de la Commission de la protection de la vie privée.
- Les personnes autorisées à accéder aux données sensibles, médicales ou judiciaires doivent être tenues au respect du caractère confidentiel des données par une obligation statutaire ou légale, ou par une obligation contractuelle équivalente (art. 25, 3° de l'arrêté royal).
- Lors de l'information de la personne concernée imposée en vertu de l'article 9 de la loi ou dans sa déclaration à la Commission (voy. *infra*), le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement des données.
- Enfin, lorsque le traitement de données sensibles ou relatives à la santé se fonde exclusivement sur le consentement par écrit de la personne concernée, le responsable du traitement doit informer la personne concernée des motifs pour lesquels ces données sont traitées ainsi que communiquer la liste des catégories de personnes ayant accès aux données.

Section 3.

Principe de transparence et droits des personnes concernées

A. Devoir d'information pesant sur les détenteurs de données à caractère personnel

1. Principe

Tout responsable de traitement de données à caractère personnel est tenu de fournir certaines informations aux personnes concernées par les données. Cette formalité doit être accomplie soit au moment de l'obtention des données, lorsque les données sont obtenues de la personne concernée elle-même, soit au plus tard au moment de la première communication des données, lorsque les données ont été obtenues de manière indirecte⁴⁷.

Les informations à fournir consistent en :

- les coordonnées du responsable du traitement (nom et adresse),
- les finalités du traitement,
- l'existence du droit de s'opposer gratuitement au traitement envisagé à des fins de *direct marketing*,
- les destinataires ou catégories de destinataires des données,
- l'existence d'un droit d'accès et de rectification des données,
- le caractère obligatoire ou non des réponses ainsi que les conséquences d'un défaut éventuel de réponse (lorsque les données sont collectées auprès de la personne concernée) et
- les catégories de données (lorsque les données sont obtenues de source indirecte).

Les quatre derniers types d'information à fournir ne doivent pas être communiqués si, compte tenu des circonstances particulières dans lesquelles le traitement est effectué, cela n'est pas nécessaire pour assurer un traitement loyal des données⁴⁸.

Lorsque les données n'ont pas été recueillies directement auprès des personnes concernées et qu'une utilisation à des fins de *direct marketing* est envisagée, le responsable a l'obligation d'informer les personnes concernées avant que les données ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers. Cela doit permettre aux personnes concernées d'exercer utilement le droit d'opposition qui leur est reconnu.

2. Exceptions

Le responsable du traitement est dispensé d'informer la personne concernée si celle-ci a déjà connaissance des informations à fournir⁴⁹. L'exception n'est valable qu'en présence de personnes déjà « informées » et non « raisonnablement supposées informées ».

⁴⁷ Art. 10 et 11 de la directive du 24 octobre 1995 et art. 9 nouveau de la loi du 8 décembre 1992.

⁴⁸ Il est à noter que la directive prévoit, de manière inversée, que les informations supplémentaires à fournir (les quatre dernières catégories d'informations) ne doivent être communiquées par le responsable que si elles sont nécessaires pour assurer un traitement loyal des données. Sur la nécessité des informations au vu du traitement loyal des données, voy. C. DE TERWANGNE et S. LOUVEAUX, « Data Protection and On Line Networks », *Computer Law & Security Report*, 1997, vol. 13, n° 4 ; M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, *op. cit.*, p. 150, n° 53.

⁴⁹ Art. 9, § 1er et § 2, al. 1er nouveau de la loi du 8 décembre 1992.

Dans les cas où les données ont été obtenues de source indirecte, les responsables de traitement de données sont en outre dispensés de fournir l'information dans deux hypothèses :

- lorsque l'information des personnes concernées se révèle impossible ou implique des efforts disproportionnés ; cette hypothèse peut apparaître notamment dans le cas de traitements à des fins statistiques ou de recherche historique ou scientifique, ou pour le dépistage motivé par la protection et la promotion de la santé publique⁵⁰. Toutefois, à la première prise de contact avec la personne concernée (mailing commercial, par exemple), les informations prévues à l'article 9, § 1^{er} devront être communiquées. En outre, le responsable doit justifier l'impossibilité invoquée dans la déclaration qu'il doit faire par ailleurs (voy. *infra*) auprès de la Commission de la protection de la vie privée ;
- si l'enregistrement ou la communication des données est effectuée en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance⁵¹.

Pour cette dernière hypothèse, la directive a en fait énoncé de façon bien plus stricte l'exception au devoir d'information. La version belge permet au pouvoir exécutif de lever l'obligation d'information, au nom sans doute d'une quelconque efficacité, sans que cela fasse l'objet d'un débat dans une assemblée parlementaire. La directive n'admet, elle, de dispenser le responsable du traitement de fournir les informations requises aux personnes concernées que « si la législation prévoit expressément l'enregistrement ou la communication des données »⁵². Il faut donc que l'enregistrement ou la communication des données soit clairement prévu par la législation.

B. Droit d'accès

1. Accès direct

Les personnes qui procèdent au traitement de données à caractère personnel sont tenues de communiquer aux personnes concernées qui le demandent la confirmation du traitement ou non de données à leur sujet, ainsi que les finalités du traitement, les catégories de données traitées et les catégories de destinataires des données⁵³.

Les responsables du traitement doivent aussi communiquer sous une forme intelligible les données faisant l'objet du traitement ainsi que toute information disponible sur l'origine des données⁵⁴. Inexistante en Belgique avant l'adaptation à la directive européenne, cette obligation d'information sur l'origine des données, qui sera logiquement d'application lorsque les données n'auront pas été recueillies directement auprès de la personne concernée, est d'un intérêt certain étant donné que c'est souvent la question de la source des informations qui préoccupe les personnes concernées.

⁵⁰ Art. 9, § 2, al. 2, *littera* a nouveau de la loi du 8 décembre 1992.

⁵¹ Art. 9, § 2, al. 2, *littera* b de la loi du 8 décembre 1992.

⁵² Art. 11, § 2 de la directive du 24 octobre 1995.

⁵³ Art. 10, § 1er, al. 1er, *littera* a nouveau de la loi du 8 décembre 1992.

⁵⁴ Art. 10, § 1er, al. 1er, *littera* b nouveau de la loi du 8 décembre 1992.

Lorsqu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, cette personne doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui sous-tend le traitement automatisé en question⁵⁵.

Pour exercer son droit d'accès, la personne concernée doit adresser une demande au responsable du traitement, envoyée par la poste ou par tout moyen de télécommunication⁵⁶. Celui-ci doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande.

Le droit d'accès offre à la personne concernée une autre voie pour obtenir des informations sur les traitements effectués sur ses données. Cette voie n'offre toutefois pas les mêmes garanties que le devoir d'information pesant sur le responsable du traitement car elle exige une démarche de la part de la personne concernée, celle-ci devant au demeurant avoir déjà connaissance de l'identité du responsable du traitement. Le droit d'accès ne compense donc pas, en termes d'information de la personne concernée sur le sort réservé à ses données, la formulation trop large de l'exception au devoir d'information présente dans la loi belge remodelée.

2. Accès indirect

En deux circonstances, la loi a prévu une formule d'accès indirect de la personne concernée à ses données.

L'accès d'une personne aux données à caractère personnel relatives à sa santé peut ainsi s'effectuer soit directement, soit par l'intermédiaire d'un professionnel des soins de santé⁵⁷ choisi par elle, si le responsable du traitement voire elle-même demande l'intervention d'un intermédiaire⁵⁸. La loi n'impose aucune motivation particulière de la part du responsable du traitement pour justifier le refus d'accès direct et la demande d'intervention d'un intermédiaire. La formule risque donc d'amener les responsables de traitements à exiger systématiquement l'accès indirect aux données médicales qu'ils contrôlent.

C'est également un accès indirect qui est mis en place pour les données faisant l'objet de traitements effectués à des fins de sûreté de l'Etat, de sécurité publique, de défense nationale, de prévention ou de répression des infractions⁵⁹. Dans ces cas, c'est par l'intermédiaire de la Commission de la protection de la vie privée que le droit d'accès peut s'exercer. Après avoir exercé ce droit, ladite Commission spécifie uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires. Cette formule d'un accès indirect systématique pour les données en question est critiquable. L'article 13 de la directive qui autorise une telle limitation au principe du droit d'accès direct ne le fait que s'il s'agit d'une mesure « nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la

⁵⁵ Art. 10, § 1er, al. 1er, *littera c* nouveau de la loi du 8 décembre 1992.

⁵⁶ Art. 32 de l'arrêté royal du 13 février 2001.

⁵⁷ La loi n'indique pas ce qu'il faut entendre par « professionnel des soins de santé ». Sur ce point voy. TH. LEONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, note 135.

⁵⁸ Art. 10, § 2 nouveau de la loi du 8 décembre 1992.

⁵⁹ Art. 13 nouveau de la loi du 8 décembre 1992.

prévention et la poursuite d'infractions pénales [...] ». Il n'est donc pas question de limitation automatique⁶⁰.

C. Droit de rectification

Toute personne concernée peut, sans frais, faire rectifier les données à caractère personnel inexactes qui se rapportent à elle et faire effacer ou interdire d'utilisation les données incomplètes ou non pertinentes au regard de la finalité du traitement⁶¹. Si des données inexactes, incomplètes ou non pertinentes ont été transmises à des tiers ou au public, le responsable doit, dans le mois qui suit l'introduction d'une requête en rectification portant sur ces données, communiquer les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées. Le responsable est cependant libéré de cette obligation lorsqu'il n'a plus connaissance des destinataires de la communication ou lorsque la notification paraît impossible ou implique des efforts disproportionnés.

D. Droit d'opposition

Désormais, en Belgique, toute personne a le droit de s'opposer à ce que les données la concernant fassent l'objet d'un traitement, pourvu qu'elle invoque des raisons sérieuses et légitimes tenant à une situation particulière. Le droit d'opposition n'est cependant pas reconnu pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat. De même, lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire, les personnes concernées ne peuvent s'opposer au traitement.

Lorsque les données sont collectées à des fins de direct marketing, la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement projeté de données à caractère personnel la concernant.⁶²

En cas d'opposition, le traitement mis en œuvre ne peut porter sur les données en cause.

E. Droit de ne pas être soumis à une décision automatisée

Un nouveau droit a été introduit dans la loi belge lors de l'exercice législatif de mise en conformité avec la directive. Aux termes de l'article 12bis, « une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité ».

Toutefois, cette interdiction ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition légale ou réglementaire. Le contrat ou la disposition en question doivent contenir des mesures de garanties de la sauvegarde des

⁶⁰ Voy. Y. POULLET et B. HAVELANGE, *op. cit.*, pp. 233 et s.

⁶¹ Art. 12, § 1er, al. 1 et 5 nouveaux de la loi du 8 décembre 1992.

⁶² Pour la mise en œuvre pratique du droit d'opposition, voy. art. 34 et 35 de l'arrêté royal du 13 février 2001.

intérêts légitimes de l'intéressé. A tout le moins, celui-ci devra avoir le droit de faire valoir *utilement* son point de vue.

Section 4.

Contrôles et sanctions

A. Contrôles

1. Déclarations

Alors que la directive invitait à conférer de réels pouvoirs de décision et d'intervention aux organes nationaux spécifiques de contrôle de l'application des lois de protection des données – organes qui existaient déjà dans la plupart des Etats membres-, le législateur belge n'a pas modifié les compétences de la Commission de la protection de la vie privée. L'organe belge est toujours limité à un pouvoir d'avis.

L'outil d'information privilégié de cet organe demeure la déclaration. Préalablement à la mise en œuvre de tout traitement entièrement ou partiellement automatisés le responsable du traitement doit en faire la déclaration auprès de la Commission (art. 17, § 1^{er} de la loi) ; L'obligation de déclaration ne s'applique pas aux registres légaux ouverts à la consultation. L'arrêté royal du 13 février prévoit en outre une série de dispenses par catégorie de traitement.

2. Recours

En cas de difficultés rencontrées dans l'exercice des droits consacrés par la loi ou en cas de non-respect d'obligations découlant de la loi, la personne concernée peut adresser une plainte à la Commission de la protection de la vie privée. Cette commission ne remplit pas exactement une fonction d'organe de recours administratif, mais elle peut effectuer une mission de médiation qui amènerait le responsable du traitement à respecter les obligations que lui impose la loi. En cas d'insuccès, la Commission dénonce l'infraction constatée au procureur du Roi et peut soumettre le litige au président du tribunal de première instance⁶³.

Une action spéciale est prévue auprès du président du tribunal de première instance, siégeant comme en référé, pour les personnes qui ont vu leur demande d'accès rejetée ou à laquelle il n'a pas été donné suite dans le délai prescrit⁶⁴.

B. Sanctions pénales

La loi prévoit de multiples sanctions pénales à l'encontre de ceux qui ne respectent pas ses dispositions. C'est le cas, notamment, du responsable du traitement qui n'a pas fourni aux

⁶³ Art. 32, § 2 de la loi du 8 décembre 1992.

⁶⁴ Art. 14 de la loi du 8 décembre 1992.

personnes concernées les informations requises⁶⁵. Une sanction est également réservée au responsable qui n'a pas donné communication, dans les quarante-cinq jours de la réception d'une demande d'accès, des renseignements demandés, ou qui a donné sciemment des renseignements inexacts ou incomplets⁶⁶. Dans les deux cas le responsable est passible d'une amende allant de cent à cent mille francs.

⁶⁵ Art. 39, al. 1er, 4° nouveau de la loi du 8 décembre 1992.

⁶⁶ Art. 39, al. 1er, 5° de la loi du 8 décembre 1992.