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

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Les cabinets d'avocats et la loi sur la protection des données à caractère personnel

de Terwangne , Cécile

Published in:
Cabinet d'avocats et technologies de l'information : balises et enjeux

Publication date:
2005

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
de Terwangne , C 2005, Les cabinets d'avocats et la loi sur la protection des données à caractère personnel. dans *Cabinet d'avocats et technologies de l'information : balises et enjeux.* Cahiers du CRID, numéro 26, Académia Bruylant, Bruxelles, pp. 149-180.

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

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

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

Download date: 07. Jul. 2025

Chapitre 5. Les cabinets d'avocats et la loi sur la protection des données à caractère personnel

Cécile de Terwangne
Chargée de cours aux
Facultés Universitaires Notre-Dame de la Paix, Namur

À l'instar des cordonniers qui sont les derniers à tirer profit de leur art, les avocats seraient-ils à ranger parmi les moins respectueux de la législation de protection des données à caractère personnel ? Cette législation s'adresse à tout avocat qui a introduit un ordinateur dans son bureau ou dans celui de sa secrétaire, qui a un agenda électronique, qui a mis une caméra dans l'entrée du bâtiment ou qui, tout simplement, est demeuré adepte du seul support papier mais fait preuve d'ordre et de classement. Il n'y a certes pas lieu de croire que la législation de protection des données ne concerne que les seuls « cyber-avocats », « e.cabinets » et autres extravagants pionniers de la technique.

Cette législation a vu le jour en Belgique en 1992[1] (après une gestation de plus de vingt ans) et a été profondément modifiée en 1998[2] pour être mise en conformité avec la directive européenne du 24 octobre 1995[3] harmonisant la matière au niveau des États membres de l'Union

---

1. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993. Sur cette loi, voy. notamment M.-H. Boulanger, C. de Terwangne et Th. Léonard, « La protection de la vie privée à l'égard des traitements de données à caractère personnel. La loi du 8 décembre 1992», *J.T.*, 1993, pp. 369-388 ; J. Dumortier, F. Robben (ed.), *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer*, Brugge, Die Keure, 1995.
2. 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. Sur cette modification voy. Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999, pp. 377 et s. ; J. Dumortier, « De nieuwe wetgeving over de verwerking van persoonsgegevens », *Recente ontwikkelingen in informatica- en telecommunicatierecht*, Brugge, Die Keure, 1999, pp. 73-103 ; C. de Terwangne et S. Louveaux, « Protection des données à caractère personnel : application en Belgique de la directive européenne », in *Actualités du droit des technologies de l'information et de la communication*, coll. Formation permanente CUP, Liège, vol. 45, février 2001, pp. 5-34.
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.

européenne. Les dix-neuf arrêtés royaux pris en exécution de la première version de la loi ont été pour la plupart abrogés pour être remplacés par l'arrêté royal du 13 février 2001[4]. Quant à la loi, elle a subi de nouveaux mais légers amendements en 2002[5] et 2003[6].

On se trouve donc en présence d'un texte relativement jeune : s'il est apparu il y a moins d'une douzaine d'années, sa version actuelle n'est entrée en vigueur qu'il y a trois ans (le 1er septembre 2001), et relativement mouvant. Ajoutées au caractère passablement complexe de la matière, ces circonstances n'ont pas à ce jour été un gage de large familiarisation des avocats avec un sujet dont on les a sans doute peu entretenus durant leur formation de juriste.

Appelés progressivement à en prendre connaissance à l'avantage ou au détriment de leurs clients, les avocats sont invités à prendre conscience de ce qu'ils sont également, au titre de leurs propres activités, concernés par la loi du 8 décembre 1992 relative à la protection des données à caractère personnel.

Les pages qui suivent abordent tout d'abord la question de l'application de la loi de 1992 aux activités des cabinets d'avocats, pour ensuite voir dans un deuxième point à quelles conditions le recueil et les utilisations de données personnelles opérés par les avocats sont licites. On évoquera dans un troisième point les démarches qui s'imposent aux avocats, avant de s'attacher, dans le point suivant, à l'exercice des droits reconnus par la législation aux personnes sur qui portent les données traitées, qui n'est pas sans soulever un problème au regard de l'obligation de secret à laquelle est tenu l'avocat. On terminera cette analyse en se penchant sur les transferts de données personnelles hors des frontières du pays.

---

31. Sur cette directive, voy. M.-H. BOULANGER, C. DE TERWANGNE, Th. LÉONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, « La protection des données à caractère personnel en droit communautaire », *J.T. dr. eur.*, 1997, pp. 121-127 (Partie 1), pp. 145-155 (Partie 2), pp. 173-179 (Partie 3).

4. 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. Sur cet arrêté, voy. C. DE TERWANGNE et S. LOUVEAUX, « Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, pp. 457-469.

5. Loi du 22 août 2002 relative aux droits du patient, *M.B.*, 26 septembre 2002.

6. Loi du 26 février 2003 modifiant 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 la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée, *M.B.*, 26 juin 2003.

1. LA LOI DU 8 DÉCEMBRE 1992 S'APPLIQUE-T-ELLE À L'ACTIVITÉ D'UN CABINET D'AVOCATS ?

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel s'applique dès que l'on se trouve en présence d'un traitement de données à caractère personnel.

1.1. Les données à caractère personnel

Est considérée comme donnée à caractère personnel toute information se rapportant à une personne physique identifiée ou identifiable[7]. La loi s'applique donc à l'égard de n'importe quelle information pourvu que celle-ci puisse être rattachée directement ou indirectement à un individu. Cela signifie que cette loi a une portée bien plus large que ce que son intitulé laisse entendre. Il ne s'agit pas de limiter l'objet de la loi à la protection de la vie privée au sens « classique » du terme[8], ce qui conduirait à ce que la loi ne s'applique qu'aux données liées à une certaine intimité de la personne. Même les données communément qualifiées de « publiques » parce que librement accessibles dans des registres publics tels l'annuaire téléphonique[9], et les données relatives à la vie professionnelle ou à des activités commerciales, tombent dans le champ de la loi pourtant généralement appelée en abrégé « loi vie privée »[10].

---

7. Article 1, § 1 de la loi du 8 décembre 1992.

8. Même si les juristes ne se sont jamais accordés sur une définition unanime de la notion de vie privée, et même si les contours de cette dernière sont mouvants dans le temps et dans l'espace, les termes « vie privée » sont couramment employés dans le sens de l'intimité d'un individu, de sa face cachée.

9. Dans sa première version, la loi excluait de son champ d'application les données faisant l'objet d'une publicité en vertu d'une disposition légale ou réglementaire et les données dont la personne à laquelle elles se rapportent assurait la publicité, pour autant que le traitement effectué sur ces données respectât les finalités de cette publicité (ancien art. 3, § 2). On était donc légitimé à parler de « données publiques », pas ou peu protégées.

10. En fait, 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 personnel. La vie privée c'est la maîtrise par chacun de son image informationnelle. 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. LÉONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », in F. RIGAUX, *La vie privée : une liberté parmi les autres ?*, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.

La seule limite à la définition réside dans le fait que les données doivent se rapporter à des personnes physiques. À la différence des lois luxembourgeoise ou italienne notamment, la loi belge ne se soucie pas des données relatives aux personnes morales. Les individus doivent être identifiés ou identifiables. Peu importe qu'ils aient ou non la nationalité belge et qu'ils résident ou non en Belgique.

Ainsi, toutes les informations qu'un avocat détient sur ses clients et ses adversaires (personnes physiques) sont visées par la loi, qu'il s'agisse d'information sur un crédit impayé, un licenciement, un vol en grande surface ou un adultère. De même, les coordonnées professionnelles de confrères ou de magistrats et les données nécessaires à la comptabilité du cabinet sont à considérer comme « données à caractère personnel ».

1.2 .Les traitements de données

Toutes les données à caractère personnel dont question au point précédent ne sont couvertes par la loi que pour autant qu'elles fassent l'objet d'un traitement[11]. En clair, il suffit qu'une opération soit appliquée aux données en faisant intervenir, ne fût-ce qu'en partie, des moyens automatisés. La notion d' « opération » est une notion ouverte et revient à peu près à tout ce que l'on peut faire avec une information. La loi énumère à titre d'exemple 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[12].

Conserver sur ordinateur des informations sur les clients, établir les procès-verbaux des réunions en indiquant le nom des participants, indiquer le nom des membres du cabinet sur le site Internet, envoyer un courrier général pour annoncer une activité, sont autant de traitements de données.

La loi s'applique dès lors que recours est fait, à un moment ou à un autre, à des moyens automatisés. Les moyens automatisés englobent

---

11. Article 3, § 1er de la loi.

12. Article 1, § 2 de la loi. 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.

toutes les technologies de l'information : informatique, télématique, réseaux de télécommunication.

Dans l'hypothèse où aucun moyen automatisé n'intervient (support papier, enregistrement sur bande magnétique, conservation sur microfiches), la loi devra quand même être respectée si les informations figurent ou sont destinées à figurer dans un fichier. Le fichier se caractérise par la classification des données personnelles qu'il contient. Il se définit comme 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 »[13]. Cette classification des données le distingue donc du dossier qui, lui, n'est pas couvert par la loi. Le critère de distinction entre fichier et dossier se situe dans le degré d'accessibilité des données contenues. Ces données doivent être 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). Un rassemblement de données non structurées et sur papier correspond à un dossier[14]. Les dossiers de clients tenus par les avocats n'échappent quant à eux à la loi que dans l'hypothèse où les pièces rassemblées sont exclusivement sur papier (ou microfiches ou bandes magnétiques) et ne font pas l'objet d'un classement permettant d'accéder de façon systématique aux données.

1.3. La localisation du responsable du traitement

La loi du 8 décembre 1992 s'applique lorsque le responsable du traitement est établi sur le sol belge ou utilise des moyens localisés en Belgique pour traiter des données à caractère personnel.

---

13. Article 1er, § 3 de la loi.

14. La différence entre fichier et dossier a 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. LÉONARD, « La protection des données à caractère personnel et l'entreprise », in *Guide juridique de l'entreprise*, 2e 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.

1.3.1. Qui est le responsable du traitement ?

Il convient de déterminer tout d'abord qui est le responsable du traitement (appelé « maître du fichier » jusqu'à la révision de la loi en 1998).

La loi ne donne pas une réponse systématique à la question de la désignation du responsable. En revanche, elle fournit les critères permettant d'identifier ce dernier. D'après l'article 4, § 1er de la loi, le responsable du traitement est la personne qui, seule ou conjointement avec d'autres, détermine les objectifs et les moyens de ce traitement de données. Il peut s'agir d'une personne physique ou morale ou même d'une association de fait. Il convient de signaler que, en dépit de la possibilité reconnue par la loi de désigner une association de fait comme responsable d'un traitement, il n'est pas nécessairement souhaitable de procéder de la sorte. En effet, si ne pas avoir de personnalité juridique propre n'empêche pas d'avoir la qualité de responsable de traitement, une telle solution conduit à des difficultés en cas de non respect des dispositions de la loi, étant donné que la loi rend le responsable du traitement civilement voire pénalement responsable du non-respect. Il conviendra dans de tels cas de se tourner vers les personnes juridiquement responsables derrière l'écran de l'association de fait.

Étant donné que la qualité de responsable du traitement dépend des deux critères énoncés ci-dessus, la désignation concrète des responsables de traitement est affaire de cas par cas. Au sein d'un cabinet d'avocats, on sera attentif à l'organisation du cabinet (structure avec réseau commun, par exemple, ou juxtaposition d'activités individuelles indépendantes) pour être à même d'identifier les responsables des différents traitements.

Il est à noter qu'il se peut que l'on désigne plusieurs co-responsables d'un traitement selon que plusieurs intervenants définissent les finalités ou les moyens de celui-ci.

On précisera encore que le rôle de responsable du traitement est essentiel dans la mesure où c'est à lui qu'incombe la majeure partie des obligations établies par la loi et c'est lui l'interlocuteur privilégié des personnes concernées par les données traitées.

1.3.2. Le lieu d'établissement du responsable du traitement

La loi du 8 décembre 1992 s'applique lorsque les données sont traitées dans le cadre des activités d'un établissement fixe du responsable du

traitement localisé sur le territoire belge[15]. L'établissement sur le sol belge suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique d'un tel établissement importe peu. Il peut s'agir d'une simple succursale ou d'une filiale ayant la personnalité juridique[16].

Un cabinet d'avocats faisant partie d'une structure « internationale » présente dans plusieurs États devra tout de même respecter la loi belge pour les activités déployées dans l'entité établie sur le territoire belge. La dépendance de ce cabinet à l'égard d'une entité mère ou son intégration complète dans une société de droit étranger est sans incidence sur la règle d'application de la loi belge de protection des données.

Par ailleurs, la loi s'applique également lorsque le responsable du traitement n'est pas établi en Belgique mais recourt à des moyens situés sur le territoire belge pour traiter des données à caractère personnel[17]. La désignation d'un responsable du traitement localisé à l'étranger mais recueillant des données en Belgique en utilisant des moyens situés dans le pays, par exemple en ayant accès via un réseau électronique aux données concernant les associés ou les collaborateurs du cabinet, ne permet donc pas d'échapper à la loi.

2. LES TRAITEMENTS DE DONNÉES PERSONNELLES OPÉRÉS DANS UN CABINET D'AVOCATS SONT-ILS LICITES ?

Pour être admissibles aux yeux de la loi de 1992, les traitements de données opérés dans un cabinet d'avocats doivent répondre à plusieurs conditions. Ces conditions tiennent d'une part aux traitements eux-mêmes (point 2.1.) et d'autre part aux données traitées (point 2.2.). Le non-respect de chacune des conditions présentées ci-dessous est punissable pénalement : d'une amende et/ou d'un emprisonnement en cas de récidive.

---

15. … Ou en un lieu où la loi belge s'applique en vertu du droit international public (art. 3 *bis* de la loi).

16. Considérant 19 de la directive 95/46.

17. 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).

2.1. Conditions de licéité portant sur les traitements

2.1.1. Traitement loyal

La première condition découle de la préoccupation de transparence que l'on souhaitait garantir afin de permettre aux individus d'avoir connaissance des opérations effectuées avec les données les concernant. Le traitement doit être loyal[18].

Cela signifie que l'on ne peut recueillir des informations sur une personne à son insu[19] ni communiquer des données, les consulter ou les utiliser si cela ne correspond pas à ce à quoi peut s'attendre l'intéressé ni faire croire que l'on poursuit un but alors qu'on a l'intention de faire autre chose avec les informations recueillies.

2.2.2. Traitement licite

Le traitement opéré sur les données doit être licite[20], c'est-à-dire qu'il doit se faire dans le respect du droit. D'autres dispositions légales que la loi du 8 décembre 1992 doivent donc éventuellement être respectées en sus.

Dans le cas des activités d'un cabinet d'avocats, il est évident qu'une série de dispositions légales et déontologiques doivent être observées lorsque l'on songe à traiter des données. La plus importante est sans doute celle imposant le respect du secret professionnel. Pour que le traitement de données soit licite, il ne doit pas impliquer une violation du secret professionnel.

2.1.3. Poursuivre un(des) but(s) déterminé(s), explicite(s) et légitime(s)

Cette troisième condition est l'expression d'un principe fondamental de la protection des données : le principe de finalité. Ainsi, les données à caractère personnel ne peuvent être recueillies qu'en vue d'une (ou de plusieurs) finalité(s) déterminée(s), explicite(s) et légitime(s) [21].

Le ou les objectifs devant être **déterminés**, il n'est pas question de collecter des données personnelles ou de décider d'utiliser de telles données sans un but précis. C'est ce but décidé au départ qui orientera

---

18. Article 4, § 1, 1° de la loi.
19. Ce qui n'empêche pas que l'on obtienne des données de tiers mais on est tenu dans ce cas de prévenir les personnes concernées de ce qu'on est en possession des données (à moins d'être dispensé de cette obligation). Voy. *infra* l'obligation d'information et les exceptions admises.
20. Article 4, § 1, 1° de la loi.
21. Article 4, § 1, 2° de la loi.

d'ailleurs toute la suite des opérations. C'est en fonction de l'objectif poursuivi que l'on saura quelles données on peut collecter, ce que l'on peut faire avec ces données, si on peut les communiquer et à qui, etc.[22]

La finalité ne peut en outre être secrète, camouflée. À moins d'être évidente, elle doit être clairement **annoncée**, soit lors de la formalité d'information[23], soit au sein de la déclaration qui doit être déposée auprès de la Commission de la protection de la vie privée[24].

Enfin, pour être considérée comme licite, la finalité que l'on poursuit en traitant des données personnelles doit être **légitime**. 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 traitement[25]. La notion de légitimité invite donc à un examen de proportionnalité[26]. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées.

Les données ne peuvent être utilisées que conformément à ce ou ces objectifs initiaux ou dans la mesure où cela est **compatible** avec ces objectifs. 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

---

22. C. DE TERWANGNE, « La protection des données personnelles en Belgique », publié sur le site de la Commission de la protection de la vie privée à l'adresse http://www.privacy.fgov.be

23. Voy. *infra*, point 3.1.

24. Voy. *infra*, point 3.2.

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

26. Voy. la position de la Commission européenne dans le même sens, dans l'arrêt *Österreichischer Rundfunk,* où la Commission évoque « l'examen de proportionnalité effectué en vertu de l'article 6, paragraphe 1, sous b) [disposition équivalant textuellement à l'article 4, § 1er, 2° de la loi belge] » (*C.J.C.E.*, arrêt du 20 mai 2003, *Österreichischer Rundfunk e.a.,* C-465/00, C-138/01 et C-139/01, point 57). La Cour de Justice des Communautés européennes arrive à une solution similaire puisqu'elle estime que sont légitimes les objectifs listés dans l'énumération de l'article 8, § 2 de la Convention européenne des droits de l'homme (objectifs qui peuvent justifier des atteintes à la vie privée), mais qu'il convient de vérifier le respect de l'exigence de proportionnalité contenue elle aussi à l'article 8, § 2 CEDH (arrêt *Österreichischer Rundfunk,* points 81 et s).

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.

La pratique développée dans les barreaux de recourir à la sous-traitance pour l'ensemble ou une partie d'un dossier ne pourra être considérée comme compatible avec la finalité de gestion du dossier confié à l'avocat initial que si le client concerné a connaissance d'une telle démarche et de l'identité du sous-traitant. Cela est d'autant plus vrai que la relation liant un client à l'avocat qu'il choisit est une relation *intuitu personae* marquée par la confiance[27]. Par contre, rien n'empêche un avocat de consulter un confrère spécialisé dans un domaine juridique particulier dès lors qu'il ne communique pas les éléments permettant d'identifier le client en cause. Il ne sera bien évidemment pas tenu d'en informer le client.

Sera également considéré comme incompatible le fait de transmettre, que ce soit gracieusement ou contre rémunération, les coordonnées de confrères à des tiers afin de permettre des envois publicitaires. Une telle transmission sera par contre autorisée si on avait informé les confrères initialement de cette possibilité.

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. L'Exposé des motifs de la loi indique clairement cette voie. Il y est effectivement énoncé : « Afin de vérifier si un traitement est compatible avec la finalité pour laquelle les données ont été collectées, il conviendra parfois de tenir compte de dispositions légales ou réglementaires. [...] Il est évident que, si les autorités disposent déjà des données nécessaires pour [une] nouvelle finalité, elles ne sont pas obligées de redemander ces données aux personnes concernées. Dans un cas pareil également, 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. Il

27. De toute manière, un devoir d'information impose d'indiquer à la personne concernée les destinataires de ses données. Voy. *infra*.

convient cependant d'observer que l'information de la personne concernée n'est pas obligatoire si l'enregistrement ou la communication des données à caractère personnel sont prévus par la loi (considérant 40 de la directive)»[28]. Pour que le traitement puisse être qualifié de compatible en s'appuyant sur des dispositions légales ou réglementaires, il faut donc que ces dispositions permettent aux personnes concernées d'entrevoir ce qui est fait avec leurs données.

2.1.4. Avoir un fondement légitime

La loi énonce les six uniques hypothèses dans lesquelles les traitements de données sont admis car reposant sur un fondement légitime.

La première hypothèse envisageable dans le contexte d'activités d'un cabinet d'avocats est celle du **consentement** de la personne concernée[29]. Pour être valable, le consentement doit être libre, informé et spécifique[30]. Il doit donc être obtenu sans pression, en connaissance de cause (la personne concernée doit notamment se rendre compte des destinataires de ses données) et ne peut être général. Le consentement ne doit pas nécessairement être exprès mais, même tacite, il doit être indubitable. Si un cabinet d'avocats décide de développer un site internet, par exemple, il conviendra d'obtenir le consentement de chaque membre du cabinet présenté nominativement sur le site[31].

D'autres hypothèses sont admises, dans lesquelles on peut se passer du consentement des personnes concernées.

Le consentement des clients, par exemple, ne doit pas être obtenu car on peut traiter des données relatives à une personne physique lorsque cela 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[32]. Entrent clairement dans cette hypothèse les traitements effectués dans le cadre de la relation liant l'avocat à son client. Cela couvre même les hypothèses de remplacement de l'avocat aux audiences, dès lors que ces remplacements permettent une bonne exécution du contrat. Notons

---

28. 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, Exposé des motifs, *Doc. parl.*, Ch. Repr., sess. ord. 1997-1998, 1566/1-n° 1, pp. 29 et 30.

29. Article 5, alinéa 1e, *littera* a.

30. Article 1, § 8 de la loi.

31. Voy. C. DE TERWANGNE, « Affaire Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous *C.J.C.E.*, arrêt du 6 novembre 2003, *Revue du Droit des Technologies de l'Information (R.D.T.I.)*, 2004, n° 19, p. 95.

32. Aricle. 5, alinéa 1er, *littera* b de la loi du 8 décembre 1992.

cependant que cette hypothèse n'autorise pas à traiter des données relatives à des individus qui ne sont pas eux-mêmes clients de l'avocat. On ne peut dès lors s'appuyer sur ce fondement pour recueillir des informations sur la partie adverse.

Il est intéressant de s'arrêter à ce stade à une pratique grandissante au sein des cabinets d'avocats, consistant à mettre les dossiers ouverts par les différents membres du cabinet sur un réseau électronique interne accessible par chacun. Cette pratique peut être partiellement couverte par les nécessités de l'exécution du contrat liant un des avocats à un client. Ainsi, le dossier peut être mis en partage sur le réseau pour les divers avocats intervenant dans son traitement (dans le cas où plusieurs avocats interviennent, mais le client doit être mis au courant de cela[33]) : il s'agit de prévoir des accès identifiés au réseau avec autorisation pour telles personnes d'accéder à telle partie du réseau hébergeant leur dossier commun. Par contre, mettre toutes les pièces d'un dossier à disposition sur un réseau interne afin de permettre une réutilisation par les collaborateurs du travail effectué par l'un d'entre eux (reprise de conclusions, par exemple) ne peut être considéré comme « nécessaire à l'exécution du contrat » établi avec le client concerné par le dossier. Pour que cette pratique soit légitime au regard de la loi du 8 décembre 1992[34], il faut soit que le client donne son accord pour procéder de la sorte, soit anonymiser le dossier avant de le déposer sur le réseau.

Pour légitimer les traitements de données de tiers (non clients), l'avocat peut invoquer deux justifications différentes.

Le traitement de données est admis s'il est nécessaire pour réaliser un **intérêt légitime** du responsable ou du tiers à qui les données sont communiquées, **à condition que l'intérêt ou les droits de la personne concernée ne prévalent pas**. L'avocat est invité dans cette hypothèse à mettre en balance l'intérêt qu'il poursuit et l'intérêt du tiers (la partie adverse, notamment) à ce que ses informations ne soient pas recueillies ou utilisées par l'avocat. Il est clair que dans la plupart des cas, même si la partie adverse n'a pas intérêt à ce que des données la concernant puisse servir l'argumentation de « l'autre bord », la défense du client et la recherche de la vérité sont des intérêts qui pèseront suffisamment lourd pour autoriser l'avocat à traiter ces données.

---

33. Voy. *infra* le devoir d'information.

34. On ne se prononcera pas dans ces pages sur la question du respect du secret professionnel au regard de ces partages électroniques de dossiers. Cette problématique est abordée par J.-P. TRIAILLE dans sa contribution au présent ouvrage.

On pourrait par ailleurs envisager que l'avocat appuie son traitement de données de tiers sur une autre hypothèse admise par la loi de 1992. Cette loi stipule en effet que des données peuvent faire l'objet d'un traitement si celui-ci 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 »[35]. Ne peut-on concevoir que l'avocat est investi d'une mission d'intérêt public, lui l'auxiliaire de la justice qui ne peut être réduit au simple défenseur d'intérêts privés ? À lire l'article 444 du Code judiciaire on l'envisage aisément. Cet article dispose que « Les avocats exercent librement leur ministère pour la défense de la justice et de la vérité ». Outre l'évocation d'une « charge à remplir »[36], la disposition confirme l'enjeu d'intérêt public lié à la profession d'avocat[37].

Enfin, les avocats peuvent traiter des données à caractère personnel lorsque cela est « 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** »[38]. L'obligation de communication d'informations (« déclaration de soupçon ») sur les clients soupçonnés de participation au blanchiment de capitaux ou au financement du terrorisme, imposée par la loi du 12 janvier 2004[39] correspond à cette hypothèse. De même que l'obligation de communication à l'ONSS de multiples informations concernant les employés salariés du cabinet.

2.2. Conditions de licéité portant sur les données

2.2.1. Conditions relatives à la qualité des données

Aux termes de l'article 4, § 1er, 3° de la loi, les données à caractère personnel faisant l'objet d'un traitement doivent être adéquates et pertinentes au regard des finalités pour lesquelles elles sont obtenues

35. Aricle. 5, alinéa 1er, *littera* e de la loi du 8 décembre 1992.

36. Pour reprendre la définition donnée par le dictionnaire Robert à « ministère ».

37. D'autres dispositions peuvent encore étayer la conception d'une mission d'intérêt public mise à charge des avocats, notamment, et de façon très éclairante, l'article 446 du Code judiciaire.

38. Article 5, alinéa 1er, *littera* c de la loi du 8 décembre 1992.

39. Loi du 12 janvier 2004 modifiant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit et la loi du 6 avril 1995 relative au statut des entreprises d'investissement et à leur contrôle, aux intermédiaires financiers et conseillers en placements, *M.B.*, 23 janvier 2004. Cette loi fait l'objet d'un recours en annulation auprès de la Cour d'arbitrage.

et pour lesquelles elles sont traitées ultérieurement. On ne peut donc traiter que les données qui présentent un lien de nécessité avec les finalités poursuivies. En outre, les données doivent être « non excessives ». On retrouve ici la règle de proportionnalité. Des données pertinentes au regard de l'objectif poursuivi mais induisant une atteinte excessive à la personne concernée par rapport à l'intérêt qu'elles présentent pour la personne qui souhaite les traiter, ne peuvent être recueillies.

Les données doivent par ailleurs 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 [40].

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[41].

2.2.2. Conditions relatives à la nature des données

2.2.2.1. Principe

Une série de données à caractère personnel ont été qualifiées de « sensibles » par la Convention n° 108 du Conseil de l'Europe[42] car elles sont susceptibles, par leur nature, de porter atteinte aux libertés fondamentales et notamment à la vie privée des personnes concernées ou d'être à la base de discriminations. Cette catégorie de données a été reprise dans la directive européenne de 1995[43] et dès lors dans la loi belge.

Il s'agit tout d'abord des données « sensibles » proprement dites, définies à l'article 6 de la loi de 1992 comme étant les données à

---

40. L'article 16, § 2 de la loi impose au responsable de traitement de 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 de la Loi.

41. Voy. le chapitre. II de l'arrêté royal du 13 février 2001, précité.

42. Article 6 de la Convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

43. Article 8 de la directive du 24 octobre 1995.

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 sexuelle[44]. L'article 7 vise, lui, les données à caractère personnel relatives à la santé. L'article 8 de la loi évoque les données communément mais improprement qualifiées de « 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 catégorie ne couvre donc pas les données traitées par les avocats pour la résolution de litiges non (encore) soumis aux tribunaux.

Le traitement des données visées aux articles 6 à 8 de la loi est en principe interdit.

2.2.2.2. Exceptions

La loi prévoit des cas dans lesquels le traitement des données tant sensibles que médicales et « judiciaires » est admis, mais en satisfaisant aux conditions supplémentaires fixées par le Roi dans l'arrêté du 13 février 2001. Certaines de ces exceptions intéressent particulièrement l'activité des avocats et leur permettront de recueillir et traiter de telles données dans le cadre de leur vie professionnelle.

À la différence des données relatives à des litiges, des suspicions, des poursuites et des condamnations, les **données sensibles et les données relatives à la santé** peuvent être traitées avec le consentement écrit de la personne concernée[45]. Il est à noter que cette exception n'est 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

---

44. Voy. les développements consacrés par Yves POULLET et Thierry LÉONARD à la portée de cette définition, liée au changement de terminologie entre l'ancienne version (qui évoquait les données « relatives à … ») et la version résultant de la modification de 1998 (données « qui révèlent »), ainsi que la critique que ces auteurs émettent en déplorant qu'on ne tienne pas plutôt compte de l'objectif des traitements effectués sur ces données pour déterminer leur caractère sensible ou non : Y. POULLET, Th. LÉONARD, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, p. 386.

45. Articles 6, § 2, *littera* a et 7, § 2, *littera* a de la loi. On rappelle que pour être valable, le consentement doit être émis librement, doit être spécifique et informé.

tout de même admis comme justifiant le traitement si celui-ci vise à octroyer un avantage à la personne concernée[46].

Les données sensibles et les données relatives à la santé peuvent en outre être traitées si le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice[47]. Cette exception permet à l'avocat de traiter des données concernant son client mais également concernant des tiers.

Les avocats peuvent également traiter des données de ces deux premières catégories lorsqu'elles ont été manifestement rendues publiques par la personne concernée[48], ou si le traitement est rendu obligatoire par une norme législative pour un motif important d'intérêt public[49].

Selon l'organisation des relations au sein du cabinet d'avocats, l'application du droit du travail impliquera peut-être le traitement de données sensibles ou médicales (gestion des congés de maladie du personnel salarié, par exemple). Le responsable du traitement bénéficiera alors de l'exception pour les traitements rendus nécessaires au vu des obligations et des droits du responsable du traitement en matière de droit du travail[50].

Signalons deux exigences de la loi qui risquent de soulever des difficultés au vu de la pratique des avocats :

– Le traitement des données à caractère personnel relatives à la santé peut uniquement être effectué sous la responsabilité d'un professionnel des soins de santé, à moins d'un consentement écrit de la personne concernée ou à moins d'être dans le cas où le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée[51]. Même si l'on ne cerne pas clairement ce qu'il faut entendre par « sous la responsabilité » d'un professionnel des soins de santé[52], on comprend que la loi impose l'intervention d'un tel professionnel chaque fois qu'un avocat traite des informations de nature

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

47. Articles 6, § 2, *littera* f de la loi et 7, § 2, *littera* i de la loi.

48. Articles 6, § 2, *littera* e et 7, § 2, *littera* h de la loi.

49. Articles 6, § 2, *littera* l et 7, § 2, *littera* e de la loi. Notez l'étonnante différence d'énonciation de cette exception dans les deux dispositions.

50. Articles 6, § 2, *littera* b et 7, § 2, *littera* b de la loi.

51. Article 7, § 4 de la loi.

52. À ce sujet voy. J. Herveg, M.-N. VERHAEGEN et Y. POULLET, « Les droits du patient face au traitement informatisé de ses données dans une finalité thérapeutique: les conditions d'une alliance entre informatique, vie privée et santé », *Rev. Dr. Santé*, 2002-2003, p. 64.

médicale[53]. Il ne peut contourner cette exigence qu'avec le consentement écrit de la personne sur qui portent les informations. Or, il est clair que si, par exemple, une cliente communique à son avocat des informations d'ordre médical sur son mari, l'avocat n'obtiendra plus que vraisemblablement pas le consentement du mari en question pour traiter ses données. Dans ce cas, il est tenu d'effectuer ce traitement sous la responsabilité d'un professionnel de la santé. Cela pourrait signifier qu'il doit s'adresser à son conseiller technique pour indiquer le sens, la portée et la fiabilité des données médicales recueillies.

– Par ailleurs, les données relatives à la santé ne peuvent être collectées qu'auprès de la personne concernée[54]. La loi admet qu'elles soient collectées auprès de tiers lorsque le traitement est effectué sous la responsabilité d'un professionnel des soins de santé (sauf si le responsable du traitement bénéficie d'une exception à cet égard) et dans la mesure où les données relatives à la santé sont nécessaires aux fins du traitement ou que la personne concernée n'est pas en mesure de fournir les données elle-même. Cette exigence vient renforcer l'importance pour un avocat de traiter des données médicales sous la responsabilité d'un professionnel de la santé, étant donné le nombre d'hypothèses où les avocats sont intéressés à recevoir de telles données sans s'adresser à la personne concernée.

Quant aux **données relatives à des litiges soumis aux cours et tribunaux, des suspicions, des poursuites et des condamnations**, elles ne peuvent faire l'objet d'un traitement que dans cinq hypothèses (alors que les deux premières catégories bénéficient de respectivement douze et dix hypothèses d'exceptions). Les avocats sont principalement appelés à appliquer l'exception leur permettant de traiter des données de cette troisième catégorie « pour autant que la défense de leurs clients l'exige »[55]. Une autre exception est sans doute également d'intérêt pour eux, celle accordée pour les traitements nécessaires à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Correspond à cette dernière hypothèse la communication de données effectuée en application de l'obligation incombant aux dépositaires d'un secret

53. La C.J.C.E. a établi qu'il convenait de réserver une interprétation large à l'expression « données relatives à la santé ». Cela conduit à faire entrer dans cette catégorie les informations portant sur « tous les aspects, tant physiques que psychiques, de la santé d'une personne » (*C.J.C.E.*, arrêt du 6 novembre 2003, *Lindqvist c. Suède*, par. 50).

54. Article 7, § 5 de la loi.

55. Article 8, § 2 *littera* d de la loi.

professionnel, en vertu de l'article 458*bis* du Code pénal, de dénoncer certaines infractions dont ils ont connaissance, commises à l'encontre d'un mineur.

Pour toutes ces hypothèses d'exceptions énoncées aux articles 6, 7 et 8 de la loi, 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 » (les secrétaires, notamment) 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.

3. DÉMARCHES À ACCOMPLIR

Les avocats ou cabinets responsables de traitements de données seront attentifs à accomplir plusieurs démarches avant de démarrer un traitement (obligation de déclaration, voy. point 3.1.) et dans le cours du traitement (obligation d'information, voy. point 3.2., et de mesures de sécurité, voy. point 3.3.). Ils feront preuve de d'autant plus de diligence que les trois obligations sont sanctionnées pénalement[56].

56. Articles 38 et 39 de la loi.

3.1. Déclarer les traitements à la Commission de la Protection de la vie privée

3.1.1. Principe

La première formalité à effectuer découle du principe de transparence, un des principes-clefs de la protection des données.

Avant de mettre en œuvre un traitement entièrement ou partiellement automatisé (avant de recueillir ou d'enregistrer des données à caractère personnel, par exemple), le responsable du traitement doit déclarer le traitement auprès de la Commission de la protection de la vie privée[57]. Il ne s'agit pas d'une demande d'autorisation, la Commission se contentant de réceptionner et enregistrer les déclarations. Ces instruments de transparence permettent tout de même à la Commission de déceler d'éventuelles irrégularités au regard de la loi : une finalité perçue comme légitime par le responsable du traitement alors qu'elle soulève une question de proportionnalité aux yeux de la Commission, des catégories de données non pertinentes au vu de la finalité déclarée, un défaut de mesures de sécurité, etc.

La Commission de la protection de la vie privée met à la disposition de tout intéressé un formulaire type (sur papier ou en ligne) permettant d'effectuer la déclaration. Une contribution financière est à verser à chaque déclaration.

Tous les renseignements transmis dans la déclaration sont repris dans un registre public. Ce registre peut être librement consulté par quiconque sur place, dans les locaux de la Commission. On peut également demander à recevoir un extrait du registre.

La déclaration comporte une description des caractéristiques du traitement. Doivent y figurer notamment :

- les finalités du traitement ;
- les catégories de données traitées (pas les données elles-mêmes), avec une description particulière des données visées aux articles 6, 7 et 8 de la loi (données sensibles, médicales et « judiciaires » - voy. *supra* point 2.2.2.) ;
- les catégories de destinataires à qui les données peuvent être fournies ;

57. Article 17 de la loi.

- les garanties entourant la communication de données à des tiers ;
- les moyens par lesquels les personnes à propos desquelles des données sont traitées en seront informées ;
- les mesures prises pour faciliter l'exercice du droit d'accès ;
- les catégories de données destinées à être transmises à l'étranger et les pays de destination ;

la période au-delà de laquelle les données ne peuvent plus être gardées, utilisées ou diffusées.

3.1.2. Exceptions à l'obligation de déclaration

Outre le fait qu'il ne faut pas déclarer les traitements manuels (sur papier ou microfiches), une série de traitements automatisés de données sont dispensés de l'obligation de déclaration[58]. Au vu du nombre de déclarations effectuées à ce jour par des avocats ou cabinets auprès de la Commission (à peine quelques-unes !), on croit volontiers que ces acteurs pensent tous bénéficier d'exemptions, à moins que ce ne soit là une manifestation de l'ignorance dans laquelle ils sont de l'existence de la loi de 1992 et des devoirs en découlant.

Il est vrai que des dispenses sont prévues[59] pour les traitements nécessaires à l'administration des salaires du personnel travaillant pour le responsable du traitement, pour les traitements qui se rapportent à la comptabilité, et pour les traitements liés à la gestion du personnel. Pour bénéficier de l'exemption de déclaration, ces derniers traitements ne doivent pas porter sur des données sensibles, médicales ou « judiciaires » (voy. *supra* point 2.2.2.) ni sur des données destinées à une évaluation des personnes concernées.

De même, ne doivent pas être déclarés les traitements de données d'identification indispensables à la communication, effectués dans le seul but d'entrer en contact avec l'intéressé[60]. Sont visés ici les carnets d'adresses professionnels : ils entrent dans le champ de la loi mais ne doivent pas faire l'objet d'une déclaration.

Si ces dispenses peuvent concerner certains traitements effectués dans les cabinets d'avocats, il est clair que cela ne porte pas sur l'essentiel des traitements opérés, liés aux activités de conseil et de défense de

---

58. Ces exceptions sont prévues aux articles 51 à 62 de l'arrêté royal du 13 février 2001. Elles sont également reprises dans le formulaire de déclaration proposé par la Commission de la protection de la vie privée.
59. Mais à certaines conditions, voy. les articles 51, 52 et 53 de l'arrêté royal.
60. Article 57 de l'arrêté royal.

clients. Une exemption est spécifiquement prévue pour les traitements qui visent la gestion de la clientèle mais elle ne peut être invoquée par les avocats. En effet, pour que l'exemption joue, les traitements ne peuvent « se rapporter ni à des données relatives à la santé de la personne concernée, ni à des données sensibles ou judiciaires au sens des articles 6 et 8 de la loi »[61]. Lorsque l'on se rappelle que les données « judiciaires » sont notamment celles relatives à des litiges soumis aux cours et tribunaux et aux juridictions administratives, ainsi qu'à des poursuites ayant trait à des infractions, on imagine aisément que nombre de traitements réalisés au sein des cabinets d'avocats sortent du champ de l'exception. D'autant que l'arrêté royal stipule en outre que « Dans le cadre de l'administration de la clientèle, aucune personne ne peut être enregistrée dans un traitement de données sur la base d'informations obtenues de tiers »[62].

Il convient de signaler que si le responsable de traitements est dispensé de la formalité de déclaration, il doit tout de même tenir à la disposition de toute personne qui en fait la demande les mêmes renseignements que ceux contenus dans la déclaration. Cet exercice n'est certes pas vain : il contribue à une bonne gestion interne des ressources informationnelles.

3.2. Informer les personnes concernées par les données traitées

3.2.1. Principe

Une deuxième application du principe de transparence évoqué ci-dessus fait peser sur le responsable du traitement de données à caractère personnel une obligation d'information des personnes concernées par les données. Cette formalité doit être accomplie soit au moment où l'on recueille des données, lorsque celles-ci sont obtenues de la personne concernée elle-même, soit dès l'enregistrement ou au plus tard au moment de la première communication des données, lorsque les données sont obtenues de manière indirecte[63].

Le responsable du traitement est tenu de fournir les informations suivantes :

- ses coordonnées (nom et adresse),
- les finalités du traitement,

61. Article 55 de l'arrêté royal.
62. Article 55, alinéa 4 de l'arrêté royal.
63. Article 9 de la loi.

- l'existence du droit de s'opposer gratuitement au traitement envisagé à des fins de *direct marketing* (toutes démarches de promotion),
- les destinataires ou catégories de destinataires des données (personnes à qui les données seront communiquées),
- 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 données.

Ni la loi de 1992 ni son arrêté d'exécution ne précisent la forme que doit prendre la démarche d'information. Celle-ci peut donc être adaptée aux circonstances. L'avocat peut oralement, de manière informelle lors d'un entretien qu'il a avec son client, lui communiquer les informations requises. Par ailleurs, les cabinets qui mettent à disposition sur leur site internet des formulaires à compléter ou qui invitent à s'inscrire à une *mailing list* pour recevoir une *newsletter*, par exemple, sont tenus de fournir les informations par écrit, en accompagnement des possibilités qu'ils offrent.

3.2.2. Exceptions

Le responsable du traitement est dispensé d'informer la personne concernée si celle-ci a déjà connaissance des informations à fournir[64]. Précisons que cette première exception n'est valable qu'en présence de personnes déjà « informées » et non « raisonnablement supposées informées »[65].

L'obligation d'informer toute personne concernée par des données que l'avocat traite n'est pas sans soulever une objection immédiate de la part de celui-ci. Cette obligation le conduirait à informer ses adversaires et tout tiers de ce qu'il est en possession d'informations sur leur compte. Il devrait de plus leur signaler notamment de quelles catégories de données il dispose. Cela n'est pas concevable pour mener

64. Article 9, § 1et § 2, alinéa 1er nouveau de la loi du 8 décembre 1992.

65. Voy. Y. POULLET, Th. LÉONARD, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, p. 386.

à bien la mission de défense des clients. Cela induirait de plus une violation du secret professionnel de l'avocat. La loi prévoit deux exceptions supplémentaires au devoir d'information, dont l'une pourrait permettre le travail efficace de ces indispensables auxiliaires de la justice et garantir le respect du secret professionnel.

Ainsi, mais seulement dans les cas où les données ont été obtenues de source indirecte, les responsables de traitement de données sont dispensés de fournir les informations requises dans deux hypothèses :

- lorsque l'information des personnes concernées se révèle impossible ou implique des efforts disproportionnés[66]. Toutefois, le responsable doit justifier l'impossibilité dans la déclaration qu'il doit faire par ailleurs (voy. *supra*) auprès de la Commission de la protection de la vie privée ;
- si l'enregistrement ou la communication des données est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance[67].

La première hypothèse d'exception peut être invoquée par les avocats en faisant valoir que, plutôt qu'une impossibilité matérielle telle celle qu'avaient à l'esprit les rédacteurs de la loi (on ne dispose pas de données de contact relatives aux personnes concernées), l'exception doit jouer en vertu d'une impossibilité fonctionnelle (l'information contrarierait l'œuvre de l'avocat)[68] et légale (l'information emporterait violation du secret professionnel).

Si l'avocat peut donc dans certains cas, et notamment à l'égard de l'adversaire, se dispenser d'informer les personnes physiques à propos desquelles il recueille des données de manière indirecte, il ne pourra jamais s'abstenir de fournir les informations prévues à l'article 9 quand il obtient les données directement de la personne concernée elle-même (lors d'un entretien ou par le biais d'un formulaire à remplir ou en cas de conservation des traces électroniques laissées lors d'une visite du site internet). Ce n'est que dans l'hypothèse où cette personne a déjà connaissance des informations en question qu'il n'y a plus lieu de les lui communiquer.

---

66. Article 9, § 2, alinéa 2, *littera* a de la loi du 8 décembre 1992.

67. Article 9, § 2, alinéa 2, *littera* b de la loi du 8 décembre 1992.

68. C'est une préoccupation identique qui a amené les auteurs de la deuxième version de la loi à dispenser de la formalité d'information les personnes traitant des données aux fins de journalisme ou d'expression artistique et littéraire (afin de permettre l'exercice de la liberté d'expression). La défense des droits en justice est un intérêt qui peut, lui aussi, justifier, lors d'une mise en balance avec les intérêts protégés par la loi de 1992, des dérogations à l'égard des dispositions qui le compromettraient.

3.3. Protéger les systèmes d'information

Le cabinet ou l'avocat responsable du traitement est tenu de prendre une série de mesures pour garantir la confidentialité des données traitées et la sécurité du système d'information. Ici encore, les obligations mises à charge du responsable du traitement sont sanctionnées pénalement[69].

3.3.1. Veiller à la confidentialité des données

Le responsable du traitement (cabinet ou avocat) doit veiller à ce que les personnes agissant sous son autorité n'aient la possibilité d'accéder à et d'utiliser que les seules données dont elles ont besoin pour exercer leurs fonctions[70].

Le responsable doit en outre mettre les personnes agissant sous son autorité au courant des prescrits légaux en matière de protection des données[71]. Il peut, par exemple, organiser des formations internes ou distribuer des instructions, sur support papier ou par la voie d'un intranet, destinées à mettre en oeuvre les principes légaux à respecter.

Enfin, le responsable doit veiller à ce que les personnes ayant accès aux données « judiciaires » (toutes les informations relatives aux litiges soumis aux tribunaux ainsi qu'à des infractions[72], ce qui représente assurément une grande part des données traitées par des avocats) ainsi qu'aux données sensibles et à celles relatives à la santé, soient tenues par une obligation légale ou contractuelle de confidentialité[73]. Cela concerne par exemple la secrétaire tapant les conclusions de l'avocat, l'archiviste, l'informaticien ayant accès au réseau pour en assurer la maintenance.

3.3.2. Veiller à la sécurité des systèmes d'information

Le responsable du traitement doit protéger les informations qu'il a rassemblées contre une curiosité malsaine venant de l'intérieur ou de l'extérieur ou contre des manipulations non autorisées, qu'elles soient de nature accidentelle ou qu'elles soient malintentionnées. Il doit prendre des mesures de différents ordres pour se prémunir contre la perte accidentelle de données, contre la destruction, la modification,

---

69. Article 38 de la loi.
70. Article 16, § 2, 2° de la loi.
71. Article 16, § 2, 3° de la loi.
72. Pour plus de détails sur cette notion, voy. *supra* point 2.2.2.
73. Article 25, 3° de l'arrêté royal.

l'accès ou tout autre traitement de données accidentel ou non autorisé[74].

La loi impose ainsi au responsable du traitement de prendre tout d'abord des mesures organisationnelles. Il s'agit de mesures qui sont souvent de bon sens mais qui, pourtant, dans la pratique observée chez nombre d'avocats, font parfois défaut. Au titre des mesures organisationnelles, on trouve le fait de limiter le nombre de personnes ayant accès aux données, de fermer les locaux où sont localisés les ordinateurs, d'archiver les fichiers dans des armoires fermées à clé, etc.

Le responsable est par ailleurs tenu de prendre des mesures techniques de protection. Ces mesures doivent permettre notamment de protéger les ordinateurs et bases de données contre les virus ou les intrusions (programme anti-virus très fréquemment mis à jour, *firewalls,…*). Une mesure technique de protection élémentaire consiste à instaurer des systèmes à accès autorisés *via* des noms d'utilisateur et mots de passe.

La loi exige d'atteindre, par ces mesures organisationnelles et techniques, un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels[75]. Le niveau de protection à assurer est fonction de la sensibilité des données traitées et des risques liés à l'utilisation de ces données. Plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus importantes seront les précautions à prendre. Les cabinets d'avocats abritant, du fait de leurs activités, un grand nombre de données sensibles, ils doivent adopter des mesures garantissant un haut degré de sécurité. En cas de présence de données relatives à la santé d'une personne, étant donné qu'elles sont utilisées en dehors d'un contexte médical, on exigera que leur traitement soit encadré de mesures de sécurité sévères.

3.3.3. Prévoir certaines garanties en cas de sous-traitance

Il se peut, et c'est vrai dans de nombreux cas dans l'univers des cabinets d'avocats, que l'on recoure aux services d'informaticiens pour gérer les aspects techniques des traitements de données (mise en place, alimentation et maintenance de bases de données ; création et hébergement d'un site internet, par exemple) ou à un service spécialisé pour assurer la comptabilité du cabinet. Si les personnes auxquelles on fait appel ne sont pas sous l'autorité directe du responsable du traitement de données, elles seront considérées comme sous-traitants

74. Article 16, § 4 de la loi.

75. Article 16, § 4, alinéa 2 de la loi.

aux yeux de la loi de 1992. Ce sera le cas notamment des sociétés extérieures mais également de personnes ou d'un département internes au cabinet mais ne se trouvant pas sous l'autorité du responsable, celui-ci étant par exemple un avocat et non le cabinet.

La loi définit le sous-traitant comme étant « la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données »[76].

Le responsable du traitement peut donc confier tout ou partie du traitement de données à caractère personnel à un sous-traitant. Il ne peut toutefois choisir à la légère son sous-traitant. Il est tenu de le sélectionner sérieusement : la loi ne l'autorise à contracter qu'avec un sous-traitant qui offre des garanties suffisantes au regard des mesures de sécurité technique et d'organisations relatives aux traitements de données.

Par ailleurs, il s'impose aussi de baliser les relations entre responsable du traitement et sous-traitant. Le responsable doit conclure un contrat, sur support papier ou électronique, avec le sous-traitant choisi. Dans ce contrat, le sous-traitant doit s'engager à n'agir que sur instruction du responsable du traitement et à respecter les mesures de protection prises. Le contrat doit également fixer la responsabilité du sous-traitant vis-à-vis du responsable du traitement[77].

4. LE DROIT À LA CURIOSITÉ ET LE DROIT D'ACCÈS AUX DONNÉES, UNE BRÈCHE DANS LE SECRET PROFESSIONNEL ?

L'article 10 de la loi du 8 décembre 1992 instaure ce qu'on a appelé un « droit à la curiosité »[78] et un droit d'accès aux données.

Tout individu apportant la preuve de son identité a le droit d'interroger un responsable de traitement afin de découvrir s'il détient des données sur lui. Le responsable interrogé doit confirmer ou non s'il détient des données et, si c'est le cas, il doit préciser dans quel but il

76. Article 1er, § 5 de la loi.

77. Article 16, § 1er de la loi.

78. Voy. C. DE TERWANGNE, « La protection des données personnelles en Belgique », *op. cit.*

traite les données, de quelles catégories de données il s'agit et quels sont les destinataires de ces données. Il s'agit là du droit à la curiosité.

Autre élément-clef d'un système censé assurer aux individus la connaissance, la maîtrise et le contrôle du sort réservé à leurs données, le droit d'accès aux données est lui aussi accordé aux personnes (prouvant leur identité) à propos de qui des données sont effectivement traitées. C'est un accès riche qui est mis en place par la loi car la personne concernée a droit à recevoir non seulement la communication, sous une forme intelligible, des données faisant l'objet du traitement, mais également toute information disponible sur l'origine des données en question.

Ce droit d'accès s'accompagne d'un droit de rectification en présence de données inexactes ou incomplètes et d'effacement en cas de données non pertinentes ou interdites[79]. Un droit d'opposition est également reconnu, particulièrement intéressant lorsque les données sont traitées à des fins de *direct marketing* car il peut alors s'exercer sans justification particulière[80].

Si le droit d'accès ne devait pas poser de problème quand il est invoqué par un client de l'avocat, il n'en est pas de même quand c'est la partie adverse qui souhaite l'exercer. Donner à l'adversaire tous les éléments que l'on a recueillis sur lui et lui indiquer la source de ces éléments compromettrait sans doute dans de nombreux cas le travail de défense de l'avocat. Cela représente de toute manière une violation du secret professionnel auquel est astreint l'avocat. Il en est déjà de même avec l'exercice du droit à la curiosité. Révéler à une personne que l'avocat traite des données la concernant en spécifiant les catégories de données en cause implique une violation du secret professionnel dans la mesure où la personne concernée pourra déduire des indications reçues qui s'est adressé à cet avocat.

Le secret professionnel n'est pas absolu. L'article 458 du Code pénal punit les personnes dépositaires par profession des secrets qu'on leur confie qui les révèlent, « hors le cas où [...] la loi les oblige à faire connaître ces secrets ».

Dans la matière qui nous occupe, la loi de 1992 impose au responsable du traitement de communiquer des informations aux personnes concernées qui les sollicitent et punit même pénalement celui qui ne respecte pas cette obligation ou qui ne la remplit que partiellement. La loi n'a rien prévu de particulier pour les avocats ou autres personnes

79. Article 12, § 1er de la loi.

80. Article 12, § 1er, alinéas 2 à 4 de la loi.

astreintes au secret professionnel[81]. À part le régime spécial de l'accès indirect aux traitements effectués par la police et autres services oeuvrant dans le domaine de la sécurité[82], la loi n'admet qu'une exception aux droits d'accès et de curiosité, au bénéfice des traitements effectués aux fins de journalisme ou d'expression littéraire ou artistique[83].

Les auteurs de la loi avaient bien pensé intégrer dans le texte belge la possibilité ouverte aux États membres à l'article 13 de la directive européenne 95/46 de limiter la portée des obligations de transparence (déclaration des traitements, devoir d'information, droit d'accès) dans les cas où cela est nécessaire pour sauvegarder la protection des droits et libertés d'autrui. Mais la formulation adoptée dans le projet de loi était à ce point floue qu'elle a suscité les justes critiques de la Commission de la protection de la vie privée. La version réécrite a essuyé la réprobation du Conseil d'État estimant qu'« il importe que le législateur détermine avec une relative précision les cas où cette protection [des droits et libertés des tiers] s'impose, et quand elle s'oppose à l'exercice des droits normalement reconnus. La simple reproduction, en droit interne, de la faculté reconnue aux États de légiférer en ce domaine, constitue en revanche une menace pour l'effectivité des droits garantis, puisqu'elle délègue, en fait, aux personnes tenues en principe au respect des obligations légales, l'appréciation des cas où elles en sont affranchies. Ce jugement doit être l'œuvre du législateur »[84].

Les auteurs du projet de loi préférèrent supprimer purement et simplement l'exception prévue, à défaut de trouver une formulation répondant aux exigences du Conseil d'État. Ils suivaient en cela la suggestion de ce dernier qui avait déclaré : « S'il est impossible de déterminer aujourd'hui avec un tant soit peu de précision les mesures nécessaires, il n'y a qu'à s'abstenir, fût-ce provisoirement, de légiférer dans l'attente que les rapports annuels de la Commission [de la protection de la vie privée] en fasse apparaître la nécessité »[85]. Il est évidemment dommage qu'on ait opté pour la mise en place d'un

---

81. Seul le cas de l'accès aux données relatives à la santé bénéficie d'un traitement spécifique.

82. Services listés à l'article 3, §§ 4 à 6 de la loi.

83. Voy. Th. LÉONARD et Y. POULLET qui déplorent également ce régime d'exception trop restreint, Y. POULLET, Th. LÉONARD, « La protection des données à caractère personnel en pleine (r)évolution », *op. cit.*, p. 390.

84. 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, Avis du Conseil d'État, *Doc. parl.*, Ch. Repr., sess. ord. 1997-1998, 1566/1-n° 1, pp. 195-196.

85. *Ibid.* p. 196.

système insatisfaisant dans l'espoir de mieux cerner les insatisfactions qui se seront fait jour et d'y répondre alors. D'autres législateurs européens ont été capables de pressentir le problème qui se poserait pour les personnes tenues à un secret légal et ont exempté cette catégorie de personnes des obligations liées à la transparence des traitements de données.

Au demeurant, même dans les cas où il existe une obligation légale de révéler des informations couvertes par le secret professionnel, il convient de signaler que « la difficulté est susceptible de se déplacer, notamment au regard des exigences découlant de la Convention européenne des droits de l'homme et requérant de la part du législateur lui-même et des organes d'application de la loi [...] qu'ils réalisent un 'juste équilibre' entre les valeurs en présence »[86]. Le droit d'accès aux données à caractère personnel entre clairement en conflit avec le secret professionnel. Pour résoudre ce conflit, il faut mettre en balance les valeurs protégées de part et d'autre. Il semble ne pas faire de doute que l'avocat sacrifiera la transparence des systèmes d'information et la maîtrise de l'image informationnelle sur l'autel « du bon fonctionnement de la justice »[87] et de la nécessité pour les avocats « d'inspirer une entière sécurité à ceux qui doivent se confier à eux et d'assurer le libre exercice du droit de défense »[88].

5. COMMUNICATION DE DONNÉES HORS DES FRONTIÈRES

5.1. Hors des frontières belges

Les transferts de données à caractère personnel entre pays membres de l'Union européenne et au sein de l'Espace Économique Européen sont désormais libres. Un cabinet d'avocats établi en Belgique peut donc librement envoyer des données à caractère personnel hors des frontières belges, pourvu que cela soit à destination d'un État membre de l'Union ou d'un pays de l'Espace Économique Européen.

Il y a toutefois une condition à cette communication : on ne peut transférer des données à caractère personnel que si cela est légitime aux yeux de la loi belge, c'est-à-dire si cet envoi s'impose pour réaliser

86. M. VAN DE KERCHOVE, « Fondements axiologiques du secret professionnel et de ses limites », in *Le secret professionnel* (sous la dir. de D. KIGANAHE et Y. POULLET), coll. Droit en mouvement, Bruxelles, La Charte, 2002, p. 15.

87. Cour eur. D.H., arrêt du 23 novembre 1992, *Niemietz c. Allemagne*, par. 37.

88. Cass. 23 juin 1958, *J.T.*, 1948, p. 598.

le but annoncé du traitement des données ou s'il est compatible avec ce but[89]. Un cabinet d'avocats implanté à Bruxelles peut ainsi envoyer à la succursale d'Amsterdam la liste des clients qui se sont présentés à lui afin de vérifier si le bureau d'Amsterdam n'a pas ces clients comme adversaires dans d'autres affaires et d'éviter dès lors d'éventuels conflits d'intérêts.

5.2. Hors des frontières de l'Union européenne

En dehors de l'Union européenne ou de l'Espace Économique Européen, on ne peut transférer des données personnelles qu'à deux conditions cumulatives[90] :

- que le transfert des données soit une opération répondant à la ou aux finalité(s) poursuivie(s), ou qu'il soit admis en tant qu'opération compatible avec cette ou ces finalité(s) ;
- que le transfert ait lieu à destination de pays qui assurent une protection des données correspondante à celle offerte sur le territoire de l'Union européenne.

Tout responsable de traitement qui souhaite exporter des données personnelles hors de l'Union européenne doit d'abord considérer si le pays destinataire assure un *niveau de protection adéquat* pour de telles données. Il faut retrouver les mêmes principes de protection que ceux établis dans la directive européenne. Pour évaluer la qualité de la protection offerte, il faut tenir compte de toutes les circonstances relatives à un transfert de données, notamment de la nature des données (on sera plus exigeant pour des données « judiciaires » que pour des données relatives à la carrière professionnelle des avocats), de la finalité et de la durée du traitement envisagé ainsi que des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, tout comme des règles professionnelles et des mesures de sécurité qui y sont respectées. En cas de doute, on peut s'adresser à la Commission de la protection de la vie privée pour savoir si un pays particulier offre une protection adéquate et si les transferts de données vers ce pays sont autorisés[91]. À titre indicatif, on signale que les transferts vers les États-Unis ne sont permis qu'à condition que l'organisation destinataire des données se soit publiquement engagée à observer les

89. Voy. *supra* au point 2.1.3. ce qu'il faut entendre par opération « compatible » avec la finalité du traitement.

90. Article 21 de la loi.

91. La Commission européenne a déjà constaté pour plusieurs pays qu'ils offraient un niveau de protection adéquat. Voy. à cet égard le site de la Commission à l'adresse http://europa.eu.int/comm/internal_market/privacy/adequacy_fr.htm.

principes de la « sphère de sécurité » (*safe harbor principles*) publiés par le ministère américain du Commerce[92]. Si cette condition n'est pas rencontrée, on ne peut transférer des données à caractère personnel outre-Atlantique que si l'une des exceptions est applicable.

La loi admet en effet diverses exceptions permettant de transférer des données vers des pays qui n'offrent pas un niveau de protection adéquat[93]. C'est notamment le cas si les personnes concernées donnent leur consentement indubitable *au transfert* de leurs données vers un tel pays. Le consentement devant être informé pour être valable, il est important que les personnes aient connaissance non seulement du transfert mais également du pays de destination et du déficit de protection qui attend leurs données dans ce pays. On sera attentif à ce que le consentement ne soit pas obtenu sous une quelconque pression. On est également autorisé à envoyer des données dans un pays n'offrant pas de protection adéquate lorsque *le transfert est nécessaire* pour exécuter un contrat avec la personne concernée. Il sera utile de s'interroger chaque fois sur le caractère nécessaire et non seulement utile du transfert pour que celui-ci soit légal.

Le responsable du traitement peut encore offrir lui-même, par la voie contractuelle, une protection appropriée. La protection peut ainsi être assurée au moyen d'un contrat liant celui qui envoie les données et celui qui les reçoit et contenant des garanties suffisantes au regard de la protection des données. Un modèle de contrat offrant des garanties suffisantes est proposé par la Commission européenne[94]. Il est disponible sur le site Internet de la Commission[95].

CONCLUSION

Ce texte n'a d'autre ambition que d'inviter les avocats à prendre conscience de ce qu'ils sont, comme tout acteur de la société, soumis à la législation de protection des données à caractère personnel et de ce que cela signifie pour eux en termes d'obligations et de démarches.

---

92. Décision de la Commission 2000/520/CE du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, *J.O.C.E.*, 25 août 2000, L 215, pp. 7-47.

93. Article 22 de la loi.

94. Décision de la Commission 2001/497/CE du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, *J.O.C.E.*, n° L 181 du 4 juillet 2001, pp. 19-31.

95. http://europa.eu.int/comm/internal_market/privacy/modelcontracts_fr.htm.

La législation de protection des données n'a pas été adoptée dans l'idée d'inhiber et d'interdire les traitements de données personnelles. Elle est destinée à œuvrer à l'équilibre entre nécessités de la vie économique et sociale et besoin de protection des droits et intérêts des individus, notamment leur autonomie et capacité de contrôle des informations qui circulent sur leur compte.

L'application de cette législation à l'activité des cabinets d'avocats conduit à appuyer voire renforcer la transparence à l'égard des clients, résultat qu'on ne peut sans doute qu'accueillir favorablement.

Par contre, la loi comporte des dispositions qui entrent indubitablement en conflit avec la règle du secret professionnel de l'avocat, notamment celle instaurant une obligation d'information de toutes les personnes physiques à propos desquelles on traite des données et celle garantissant à ces mêmes personnes un droit d'accès aux données que l'on détient sur elles. On a proposé dans les pages qui précèdent une lecture de l'exception admise au devoir d'information qui permette à l'avocat de s'affranchir de ce devoir sans irrégularité par rapport à la loi de 1992. Par contre, le droit d'accès ne soufre aucune exception au bénéfice des personnes obligées au secret. Même si l'interpellation d'un avocat en application de ce droit d'accès relève davantage de la conjecture que de la conjoncture, il serait temps que les instances concernées signalent à la Commission de la protection de la vie privée les difficultés suscitées par la non prise en compte par les auteurs de la loi des obligations liées au secret professionnel. Ainsi que le suggérait le Conseil d'État dans son avis sur le projet révisant la loi en 1998, la commission gardienne de la loi y ferait écho dans son rapport annuel (rapport qu'elle n'a toutefois plus publié depuis 2001…), ce qui conduirait le ministre de la Justice à proposer une révision de la loi[96].

Les avocats amenés dans leur pratique à traiter des données médicales seront peut-être confrontés à des difficultés supplémentaires découlant des conditions imposées par la loi de 1992 pour traiter des données relatives à la santé, notamment l'obligation de placer le traitement de telles données sous la responsabilité d'un professionnel des soins de santé.

96. Avis du Conseil d'État, précité, p. 196.