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

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La protection des données à caractère personnel

De Terwangne, Cécile; Rosier, Karen

Published in:
Journal du droit des jeunes : la revue d'action juridique et sociale

Publication date:
2016

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
De Terwangne, C & Rosier, K 2016, 'La protection des données à caractère personnel: un aspect incontournable de l'informatisation du social', *Journal du droit des jeunes : la revue d'action juridique et sociale*, numéro 355, pp. 7-15.

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: 03. Jul. 2025

dossier

La protection des données à caractère personnel : un aspect incontournable de l'informatisation du social

Cécile de Terwangne (1)
Karen Rosier (2)

Présentation de la législation en matière de protection des données (3)

L'informatisation de la gestion de l'information a, outre les défis techniques qu'elle soulève, amené dans son sillage la nécessité de tenir compte de la législation en matière de protection des données.

Celle-ci ne date pas d'hier. La loi relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel a été adoptée le 8 décembre 1992 (4). Elle a été profondément remaniée par la loi du 11 décembre 1998 pour transposer la 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 (5). Cette directive poursuit un double objectif : celui de permettre la libre circulation des données à caractère personnel entre États membres et au sein des États membres, d'une part, celui de préserver un niveau de protection de la vie privée des personnes physiques satisfaisant, en conformité avec les exigences de l'article 8 de la Convention Européenne des Droits de l'Homme et des Libertés Fondamentales, d'autre part.

Cette réglementation est devenue, de par l'évolution des technologies de la communication, un enjeu de société majeur. Le cadre législatif fait d'ailleurs actuellement l'objet d'une complète révision, puisque c'est un Règlement européen qui est sur le point d'être adopté et qui sera directement applicable en Belgique. À terme, la loi du 8 décembre 1992 est donc vouée à disparaître même si les principes et grands axes de la réglementation se retrouveront dans ce Règlement.

Dans le cadre de cette réforme, le rôle des autorités de contrôle nationales chargées de surveiller l'application, sur leur territoire, de la législation en matière de protection des données est appelé à être renforcé. En Belgique, il s'agit de la Commission de la Protection de la Vie Privée qui actuellement a essentiellement une compétence d'avis et de recommandation sur des problématiques particulières posées par l'application de cette loi. Ces avis et ces recommandations sont librement consultables sur le site internet de la Commission (6). Il peut donc être fait appel à cette Commission pour obtenir des précisions et explications en cas de doute sur l'application de la loi (7).

La loi du 8 décembre 1992 est complétée par d'autres réglementations plus spécifiques telles que la loi du 8 août 1983 organisant un registre national des personnes physiques, la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale (BCSS), l'arrêté royal du 5 novembre 2002 instaurant une déclaration immédiate à l'emploi, la loi du 24 février 2003 concernant la modernisation de la gestion de la sécurité sociale et concernant la communication électronique entre des entreprises et l'autorité fédérale.

Ces lois spéciales permettent d'encadrer les flux de données en réservant à certaines personnes et certaines finalités

(1) *Professeur à la Faculté de droit de l'UNamur et directrice de recherche au CRIDS*

(2) *Maître de conférences à la Faculté de droit de l'UNamur, chercheuse au Crids, Avocate*

(3) *La présente contribution reprend et actualise des passages des publications antérieures suivantes : K. Rosier, «Gestion et protection des données à caractère personnel dans la relation de travail»,* Le droit du travail à l'ère du numérique, *Limal, Anthemis, 2011, pp. 61-119. 38; J. Deumer, S. Gilson, K. Rosier, E. Dermine et M. Glorieux, «Approche transversale: Particularités de la preuve en droit de la sécurité sociale»,* Regards croisés sur la sécurité sociale, *Limal, Anthemis, 2012, pp. 382-444, C. de Terwangne, «Présentation succincte de la loi de protection des données»,* Vie privée et données à caractère personnel, *Bruxelles, Politeia, 2013, chap. 3.1., pp. 1 à 18.*

(4) *Et s'inspirait des travaux du Conseil de l'Europe qui avaient déjà dessiné les contours de cette législation dans la Convention n° 108 pour la protection des données (Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, STE n° 108, le 28 janvier 1981. Entrée en vigueur le 1er octobre 1985)).*

(5) M.B., *3 février 1999. La loi du 11 décembre 1998 transpose la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Les modifications apportées par la loi du 11 décembre 2008 à la loi du 8 décembre 1992 ne sont cependant entrées en vigueur qu'en 2001. L'entrée en vigueur était en effet subordonnée à l'adoption de mesures d'exécution dans un Arrêté royal qui ne fut promulgué que le 13 février 2001.*

(6) *www.privacycommission.be*

(7) *On soulignera encore qu'un travail de réflexion sur la manière d'appliquer la législation de la protection des données est également mené au niveau européen, notamment par le biais du Groupe dit de l'Article 29. Ce groupe, qui tient son nom du fait qu'il a été institué par l'article 29 de la directive 95/46/CE, est un organe consultatif européen, composé entre autres de représentants de chaque autorité de contrôle des États Membres et qui rend des avis publiés sur un site internet (http://ec.europa.eu/justice/policies/privacy). Les avis et autres documents de travail du Groupe de l'Article 29 et de la Commission de la Protection de la Vie Privée n'ont pas de force contraignante, mais peuvent être utiles à l'interprétation de la législation sur la protection des données.*

la possibilité de transférer ou de recevoir des informations centralisées dans des banques de données et en réglementant les modalité de ces transferts.

Le respect de ces lois spéciales est placé sous le contrôle de comités sectoriels au sein de la Commission de la Protection de la Vie privée qui doivent notamment délivrer les autorisations préalables requises pour l'accès et le transfert de certaines données. Elles sont d'ailleurs assez nombreuses dans le secteur social et de l'aide à la jeunesse.

La matière de ces lois particulières est toutefois trop vaste pour être examinée dans le cadre de la présente contribution.

On pointera cependant une particularité qui peut avoir une incidence sur la façon de traiter l'information. L'article 11 de la loi du 15 janvier 1990 – loi organique de la BCSS – prévoit que lorsque les données sociales sont disponibles dans le réseau, les institutions de sécurité sociale sont tenues de les demander exclusivement à la Banque-carrefour et qu'elles sont également tenues de s'adresser à la Banque-carrefour lorsqu'elles vérifient l'exactitude des données sociales disponibles dans le réseau. La Cour du travail de Bruxelles en a fait application dans un litige relatif à l'aide sociale [8]. Alors que le CPAS reprochait à un demandeur d'aide son manque de collaboration en ce qu'il n'avait pas fourni des informations relatives à son contrat de travail, la Cour rappelle cet article 11 et considère qu' «*un manque de collaboration du demandeur ne peut être envisagé à propos d'informations auxquelles le CPAS peut accéder, accessibles via la Banque-carrefour de la sécurité sociale*» [9].

En marge des développements consacrés ci-après à la loi du 8 décembre 1992, il convient donc de garder à l'esprit que des dispositions particulières entrent en ligne de compte pour déterminer qui peut avoir accès à quelles données, à qui on peut communiquer des données détenues par une autorité publique ou encore quelle est la source authentique à éventuellement privilégier pour l'obtention d'une donnée [10].

L'objectif de notre propos restera modeste. Il s'agira de présenter les grands axes de cette législation et des principales questions qu'elle soulève dans le cadre de l'usage de banques de données impliquant collecte, accès, partage ou encore conservation de données relatives à des personnes physiques.

Quand la loi relative à la protection des données s'applique-t-elle ?

La protection de données plus que de la vie privée

La protection qu'offre la législation relative au traitement de données à caractère personnel va au-delà de la protection de la sphère privée. En effet, cette législation entend protéger, dans certains traitements, toute donnée dès lors qu'elle a trait à une personne physique identifiée ou identifiable. Il n'est pas nécessaire de se demander si cette donnée relève ou non de sa vie privée, est ou non confidentielle ou encore si elle est par ailleurs publiquement accessible. La législation s'applique quelle que soit la réponse à ces questions.

La loi du 8 décembre 1992 s'applique à tout traitement totalement ou partiellement automatisé (par des moyens électroniques) et aux traitements manuels (travail sur des fichiers papier ou microfiches) [11] dès que, dans ce dernier cas, les données à caractère personnel sont contenues ou appelées à figurer dans un fichier.

Qu'entend-on par «donnée à caractère personnel» ?

Une donnée à caractère personnel est toute information qui concerne une personne physique identifiée ou identifiable (que l'on appelle la «personne concernée») [12].

L'*information* peut donc être de toute nature : il peut s'agir d'un nom, d'une photographie, d'une image vidéo, d'un enregistrement vocal, etc. Par ailleurs, il peut s'agir tant d'informations objectives, telles que le nom ou la situation familiale d'une personne, que de données subjectives, telles que des avis, évaluations ou appréciations se rapportant à cette personne [13]. Ainsi, la Commission de la protection de la Vie privée a-t-elle rappelé, lors de l'examen du projet d'arrêté du Gouvernement flamand relatif à l'aide intégrale à la jeunesse, que des informations sur les possibilités du mineur et de ses parents, leur vision des choses, les possibilités des prestataires de services, un plan de travail doivent être qualifiées de données à caractère personnel, puisqu'elles concernent des personnes identifiées [14].

La donnée doit concerner une *personne physique*, à l'exclusion des personnes morales (sociétés, associations, personnes de droit public...). Les informations relatives à la famille d'un individu peuvent dans certaines circonstances être considérées comme des données à caractère personnel concernant cet individu lorsqu'elles ont trait à cette personne [15]. On peut en déduire que les données relatives à la composition de la famille d'un jeune qui figurent dans son dossier sont à traiter comme les données relatives à ce jeune, par exemple.

Pour être qualifiée de «donnée à caractère personnel», l'information doit concerner une personne *identifiée ou identifiable*, peu importe la nationalité de celle-ci. Autrement dit, sont considérées comme données à caractère personnel les informations immédiatement liées à une personne identifiée ainsi que les informations relatives à une personne

(8) *C. trav. Bruxelles, 21 avril 2010, RG 51.591 et 51.809, www.cass.be.*

(9) *Ce principe est également rappelé dans un arrêt de la Cour du travail du 8 juin 2011 (C .trav. Bruxelles, 8 juin 2011, RG 2010/AB/328,* www.cass.be*).*

(10) *Voy. à ce sujet, par exemple : Ch. BURNET, «Les sources authentiques de données: l'Accord de coopération du 23 mai 2013»,* RDTI*, 2014, pp. 27-42.*

(11) *Loi du 8 décembre 1992, art. 3.*

(12) *Loi du 8 décembre 1992, art. 1, § 1er.*

(13) *Groupe de l'Article 29, «Avis 4/2007 sur le concept de données à caractère personnel», WP 136, 20 juin 2007, p. 7, http://ec.europa.eu/justice/policies/privacy.*

(14) *CPVP, avis n° 07/2014 du 5 février 2014 relatif au projet d'arrêté du Gouvernement flamand relatif à l'aide intégrale à la jeunesse, p. 4, www.privacycommission.be.*

(15) *Groupe de l'Article 29, «Avis 4/2007 sur le concept de données à caractère personnel», WP 136, 20 juin 2007, p. 11, http://ec.europa.eu/justice/policies/privacy.*

dont on ne connaît pas l'identité, mais qui pourrait, dans l'absolu, être identifiée soit par celui qui traite les données en question, soit par un tiers. Sont ainsi considérées comme données à caractère personnelles les images d'une bande vidéo même si l'on n'a pas identifié les personnes qui y apparaissent. Constituent également des données à caractère personnel les données codées c'est-à-dire les données qui ne peuvent être mise en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code [16]. La personne qui accède la donnée non nominative doit la considérer comme une donnée à caractère personnel dès lors qu'un tiers a la possibilité de retrouver l'identité de la personne concernée par la donnée en la recoupant avec le numéro d'identification.

On oppose aux données à caractère personnel les *données anonymes* c'est-à-dire les données qui ne peuvent pas ou plus être mises en relation avec une personne identifiée ou identifiable [17]. Le traitement des données anonymes n'est soumis à aucune condition légale. En revanche, les opérations par lesquelles une donnée à caractère personnel est rendue anonyme constituent un traitement de données à caractère personnel et sont soumises au respect des conditions légales.

Qu'entend-on par «*traitement de données*» ?

La notion de traitement de données à caractère personnel est très large. Elle recouvre «*toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel*» [18].

Bien que cela ne ressorte pas explicitement du texte de la loi, les termes «traitement de données» sont généralement utilisés pour désigner un ensemble d'opérations techniques qui poursuivent une ou plusieurs finalités définies. Aussi parlera-t-on du traitement de données effectué pour la gestion de la mission d'aide sociale d'un CPAS pour englober toutes les opérations (collecte, enregistrement, suppression, communication, conservation d'informations...) mises en œuvre dans le but de gérer le suivi des données des assurés sociaux concernés.

Qu'entend-on par «*fichier*» ?

Un fichier est «*tout 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*» [19]. Il peut s'agir tant d'un fichier électronique (sur ordinateur) que d'un fichier papier. Ce qui est déterminant pour la qualification de fichier papier, c'est l'existence d'une structure logique, d'un critère de classement, permettant le traitement systématique des données qui y sont contenues (consultation, diffusion, effacement...). Ainsi, un simple dossier thématique qui ne permet pas ce traitement de données systématique ne peut être qualifié de «fichier» au sens de la loi du 8 décembre 1992 [20].

Les principes clés de la protection des données

Afin d'assurer un équilibre entre la protection des données à caractère personnel et la nécessité de pouvoir traiter ces données dans le cadre de la vie économique et sociale, la législation adoptée repose essentiellement sur des principes impliquant une pondération des intérêts en présence au cas par cas. Cette approche présente l'avantage d'une régulation suffisamment abstraite pour pouvoir s'appliquer à tous les secteurs d'activités et à tous les cas de figure. Elle fait toutefois peser sur les personnes censées l'appliquer le devoir et le risque de l'application concrète des dispositions de la loi.

Ceci étant, il existe une certaine logique dans la loi qui s'articule essentiellement autour de quatre principes : finalité, légitimité et proportionnalité et transparence.

Le principe de **finalité** implique que l'utilisation de données à caractère personnel ne puisse être réalisée que pour des objectifs précis et déterminés à l'avance [21]. Les données personnelles ne peuvent être recueillies qu'en vue d'un ou de plusieurs objectifs particuliers. C'est ce but décidé au départ qui va orienter 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. On ne peut faire que ce qui répond à ou aux objectifs poursuivis et ce qui est compatible avec ces objectifs. On considère comme compatible notamment ce qui est prévu par la loi et ce que la personne concernée peut raisonnablement prévoir.

> Signalons à ce sujet que la loi contient un régime tout à fait spécifique concernant la réutilisation de données à des fins historiques, statistiques ou scientifiques qui permet de cerner dans quelles conditions des données contenues dans une base de données peuvent être ainsi réutilisées dans le cadre de projet de recherches ou d'études, notamment [22].

Par ailleurs, pour être admis, l'objectif que l'on poursuit en traitant des données personnelles doit être **légitime**. C'est-à-dire qu'un équilibre doit exister entre l'intérêt du responsable du traitement et les intérêts des personnes sur qui portent les données traitées. La loi envisage six hypothèses dans lesquelles un traitement doit impérativement s'inscrire [23]. Ces hypothèses sont *alternatives*, une de celle-ci pouvant suffire à fournir un fondement légitime pour le traitement.

Il s'agit des hypothèses suivantes :

---

(16) A.R. du 13 février 2001, art. 1, 3°.

(17) A.R. du 13 février 2001, art. 1, 5°.

(18) Loi du 8 décembre 1992, art. 1er, § 2.

(19) Loi du 8 décembre 1992, art. 1er, § 3.

(20) Cass., 16 mai 1997, J.T., 1997, p. 779.

(21) Loi du 8 décembre 1992, art. 4, 2°.

(22) Cf. 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, art. 2 et suiv.

(23) Loi du 8 décembre 1992, art. 5.

- le traitement des données est nécessaire pour exécuter une mission d'*intérêt public* ou une mission relevant de l'exercice de l'autorité publique. À ce titre, un CPAS ou un service d'aide à la jeunesse est en droit de recueillir et traiter des informations qui sont nécessaires à l'accomplissement des missions qui lui sont attribuées par la loi.
- la personne concernée a sans ambiguïté donné son *consentement.* Le consentement n'est valable que s'il est libre (c'est-à-dire s'il a été émis sans pression), spécifique (le consentement doit porter sur un traitement précis) et informé (la personne a reçu toute l'information utile sur le traitement envisagé). Le consentement ne doit pas nécessairement être donné par écrit. Dans l'hypothèse où la personne concernée est mineure, ce sont ses représentants légaux qui doivent donner ce consentement.
- le traitement est exigé par une *loi,* un décret ou une ordonnance. On pense, par exemple, à certaines dispositions du Code pénal social qui prévoient l'échange de données notamment entre les inspecteurs sociaux et des administrations ou services [24] et l'échange électronique d'information entre les acteurs de la lutte contre le travail illégal et la fraude sociale [25].
- le traitement des données est nécessaire à l'exécution d'un *contrat* ou à l'exécution de mesures précontractuelles sollicitées par la personne concernée. C'est le cas de l'enregistrement de données pour permettre la facturation d'un service.
- le traitement est nécessaire pour sauvegarder un *intérêt vital* de la personne concernée. C'est le cas de l'accidenté inconscient, à propos duquel on rassemble des données médicales (résultats de tests sanguins, notamment) afin de le soigner.
- le traitement des données est nécessaire pour réaliser un *intérêt légitime* du responsable ou d'un tiers, à condition que l'intérêt ou les droits de la personne concernée ne prévalent pas.

Le troisième principe de **proportionnalité** est directement en lien avec le premier, puisqu'en découle l'exigence d'une légitimité dans la finalité d'utilisation et également l'obligation de ne traiter que les données qui sont *nécessaires* et *pertinentes* pour réaliser la finalité déterminée [26].

Prenons l'exemple, en matière d'aide sociale, de l'article 60, § 1er de la loi organique du 8 janvier 1976 des centres publics d'action sociale. Cette disposition délimite l'objectif des démarches du CPAS : «*L'intervention du centre est, s'il est nécessaire, précédée d'une enquête sociale, se terminant par un diagnostic précis sur l'existence et l'étendue du besoin d'aide et proposant les moyens les plus appropriés d'y faire face. L'intéressé est tenu de fournir tout renseignement utile sur sa situation et d'informer le centre de tout élément nouveau susceptible d'avoir une répercussion sur l'aide qui lui est octroyée*». L'enquête est donc facultative, et son objet délimité par la finalité de l'enquête sociale : déterminer l'existence et l'ampleur de l'état de besoin. On peut donc en déduire que seules les informations pertinentes pour apprécier cet état de besoin peuvent être recherchées et traitées.

À propos de l'article 48, § 1, 1° du projet d'arrêté du Gouvernement flamand relatif à l'aide intégrale à la jeunesse qui prévoyait «*la collecte de toutes les données utiles, (...) qui sont nécessaires pour évaluer adéquatement la nécessité sociale de l'aide à la jeunesse*», la Commission de la protection de la Vie privée a constaté qu'il s'agissait d'une «*description très large, probablement dictée par le fait qu'il est difficile d'énumérer tous les éléments indiquant que l'on est confronté à une situation inquiétante*» [27]. Faisant application de ce principe de proportionnalité, elle a souligné que cela ne constituait pas «*un passe-droit permettant de demander et d'enregistrer n'importe quoi*» et qu'il incombait à la structure mandatée d'effectuer le contrôle de proportionnalité concernant toutes les données qu'elle collecte [28].

Ce principe de proportionnalité impose enfin de supprimer les données ou des rendre anonymes dès qu'elles ne sont plus nécessaires [29].

Pour assurer la **transparence** du traitement, la personne qui traite les données devra faire une déclaration du traitement auprès la Commission de la Protection de la Vie Privée [30] et fournir certaines informations aux personnes concernées [31]. Cette exigence de transparence participe à la loyauté du traitement vis-à-vis de la personne concernée par les données. [32]

Lorsque les données sont obtenues directement de la personne concernée (par exemple, via un formulaire à remplir), il faut fournir immédiatement les informations aux personnes auprès desquelles on recueille des données, à moins que ces personnes ne soient déjà informées. Il se peut également que le responsable du traitement obtienne les données auprès d'un tiers et non auprès de la personne concernée. Dans ce cas, le responsable du traitement doit informer les personnes concernées, à moins qu'elles ne le soient déjà, au moment de l'enregistrement des données ou, au plus tard, lors de la première communication à un tiers si une telle communication est envisagée [33].

Lors d'une collecte auprès de tiers, le responsable du traitement est toujours *dispensé de l'obligation* d'information dans deux hypothèses.

---

(24) Code pénal social, articles 54 et s.

(25) Code pénal social, articles 100/1 et s.

(26) L. du 8 décembre 1992, art. 4, 3°.

(27) CPVP, avis n°07/2014 du 5 février 2014 relatif au projet d'arrêté du Gouvernement flamand relatif à l'aide intégrale à la jeunesse, p. 9, www.privacycommission.be.

(28) Ibidem.

(29) L. du 8 décembre 1992, art. 4, 5°.

(30) L. du 8 décembre 1992, art. 17. Il existe cependant des exceptions à cette obligation, définies par l'arrêté royal du 13 février 2001 (A.R. du 13 février 2001, art. 51 et suiv.). Par ailleurs, cette obligation de déclaration ne sera plus d'actualité lorsque le règlement européen relatif à la protection des données entrera en vigueur (soit 2 ans après son adoption qui, rappelons-le, est imminente). Les responsables seront toutefois tenus d'élaborer un document interne contenant une description des éléments clés de chaque traitement des données, ce qui, dans les faits, correspondra au contenu de la déclaration actuelle.

(31) L. du 8 décembre 1992, art. 9.

(32) L. du 8 décembre 1992, art. 4,1°.

(33) Loi du 8 décembre 1992, art. 9, § 2.

La première concerne le cas de figure où la démarche d'information s'avère impossible ou extrêmement difficile [34].

La loi ne précise pas ce qui pourrait constituer un obstacle rendant impossible ou extrêmement difficile la fourniture d'information. On peut aisément concevoir des difficultés matérielles : le nombre de personnes concernées, le fait que l'on ne soit pas en mesure de les contacter, etc. Rien n'exclut de pouvoir également concevoir des impossibilités d'une autre nature. Ainsi, peut-on concevoir qu'un avocat, face à la question de l'information à fournir aux personnes à propos desquelles il a obtenu des données, puisse se prévaloir de l'exception en raison d'une impossibilité fonctionnelle (dans le sens où l'information contrarierait l'œuvre de l'avocat) ou légale (dans la mesure de l'existence d'une obligation légale de respecter le secret professionnel) [35]. Dans le droit fil de ce raisonnement, il nous semble que, dans d'autres hypothèses, on pourrait invoquer une impossibilité d'informer lorsque cette démarche irait à l'encontre d'une contrainte liée à l'objectif même du traitement (par exemple, dans le cadre d'une démarche protectionnelle) ou au respect du secret professionnel d'autres personnes tenues par une obligation de secret professionnel [36].

Celui qui invoque l'impossibilité ou les efforts disproportionnés qu'impliquerait pour lui le fait d'informer les personnes concernées doit se justifier auprès de la Commission de la Protection de la Vie Privée. Il rajoute cette justification dans la déclaration qu'il doit faire avant de démarrer son traitement [37].

Une seconde exemption est prévue : le responsable du traitement est exempté de l'obligation d'information lorsque 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 [38]. La loi du 8 décembre 1992 ne semble donc pas exiger que la loi, le décret ou l'ordonnance en question prévoie la communication ou l'enregistrement en tant que tels. À lire la loi du 8 décembre 1992, il suffit que cet enregistrement soit effectué pour l'application de dispositions légales. Toutefois, la directive 95/46, que la loi du 8 décembre 1992, transpose n'admet 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*». Il faut donc que l'enregistrement ou la communication des données soit clairement prévu par la législation. Cette exigence est reprise dans le texte du futur règlement européen qui remplacera incessamment la directive 95/46.

Toutefois si une prise de contact s'établit (plus tard) avec une ou plusieurs personnes concernées, le responsable du traitement devra à ce moment fournir les informations énumérées [39].

Deux obstacles au traitement de données

La problématique des transferts de données hors du territoire de l'EEE

Parmi les opérations de traitement qui peuvent être effectuées, il en est une qui est réglementée de manière particulière : il s'agit du transfert de données vers un territoire situé hors de l'Espace Économique Européen.

Les transferts de données à caractère personnel entre pays membres de l'Union européenne et au sein de l'Espace Économique Européen sont libres. Une personne établie en Belgique peut donc envoyer des données à caractère personnel dans un autre pays de l'Espace Economique Européen [40] si cet envoi est légitime aux yeux de la loi belge, c'est-à-dire si cet envoi s'impose pour réaliser le but annoncé du traitement des données ou s'il est compatible avec ce but.

En revanche, on ne peut transférer des données à caractère personnel vers des pays situés en dehors de l'Espace Economique Européen à moins que ceux-ci n'assurent une protection des données correspondante à celle assurée sur le territoire de l'Union européenne [41]. En l'absence d'une telle règle, la forte protection garantie à l'intérieur de l'Union européenne serait rapidement vide de sens, étant donné la facilité de circulation des données grâce aux nouvelles technologies.

Tout responsable de traitement qui souhaite exporter des données à caractère personnel hors de l'Espace Économique Européen doit d'abord se demander si le pays destinataire assure un *niveau de protection adéquat* pour de telles données c'est-à-dire si le tiers à qui on communique les données est soumis au respect des mêmes principes de protection que ceux établis sur le territoire européen.

Pour évaluer la qualité de la protection offerte, il faut tenir compte de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données, notamment de la nature des données, de la finalité et de la durée du ou des traitements envisagés 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.

---

(34) Loi du 8 décembre 1992, art. 9, § 2

(35) C. DE TERWANGNE, «Les cabinets d'avocats et la loi sur la protection des données à caractère personnel», in Cabinets d'avocats et technologies de l'information : balises et enjeux, *Bruxelles, Bruylant, 2005, p. 171.*

(36) À noter que la loi prévoit des exceptions générales à l'obligation d'information notamment au bénéfice des autorités publiques en vue de l'exercice de leurs missions de police judiciaire (Loi du 8 décembre 1992, art. 3, § 5, 1°).

(37) A.R. du 13 février 2001, art. 31.

(38) Loi du 8 décembre 1992, art. 9, § 2.

(39) A.R. du 13 février 2001, art. 30.

(40) Le principe de libre circulation des données au sein de l'UE a en effet étendu à l'EEE, qui inclut la Norvège, le Liechtenstein et l'Islande.

(41) Loi du 8 décembre 1992, article 21, § 1.

Le transfert de données vers des pays qui n'offrent *pas un niveau de protection adéquat* peut néanmoins être réalisé soit dans les hypothèses où la loi le prévoit, soit moyennant la réunion de garanties qui pallient l'absence de protection suffisante que nous ne développerons pas dans le cadre de la présente contribution.

La question du transfert de données mérite toutefois d'être pointée dès lors qu'elle se pose aujourd'hui de manière encore plus récurrente en raison de l'évolution des technologies qui permettent le stockage d'informations hors de l'EEE dans le cadre des services de *cloud computing*. Dans le cadre d'un tel projet d'externalisation du stockage ou de la sauvegarde de données à caractère personnel il convient donc d'être attentif au lieu où les données seront stockées par le prestataire.

Régime d'exception pour des données sensibles

Tandis que le traitement des données «ordinaires» est permis pour autant que certaines conditions prévues par la loi soient remplies, le traitement des données sensibles est quant à lui interdit sauf dans le cas des exceptions limitativement prévues par la loi [42]. Dans le cas où le traitement entre dans le champ d'application d'une de ces exceptions, il reste soumis aux mêmes conditions que le traitement des données «ordinaires».

Par données sensibles, on entend les données relatives à la race, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé, à la vie sexuelle, à des suspicions, des poursuites ou des condamnations pénales ou administratives [43].

Il est en principe interdit de collecter, d'enregistrer ou de demander communication de données telles que celles énumérées ci-dessus sauf dans des cas très spécifiques prévus par la loi et moyennant le respect de précautions supplémentaires.

À l'exception des données relatives à des suspicions, des poursuites et des condamnations, les données sensibles peuvent être traitées avec le *consentement écrit* de la personne concernée. Cela n'est toutefois pas 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 s'il permet d'octroyer un avantage à la personne concernée.

On peut également traiter ces données si cela est nécessaire *pour l'administration de soins* (le traitement doit alors se faire sous la surveillance d'un professionnel des soins de santé); lorsque le traitement est nécessaire à la promotion et à la protection de la santé publique y compris le dépistage; si le traitement est exigé par la législation sur le travail; s'il porte sur des données manifestement rendues publiques par la personne concernée (p. ex., l'appartenance politique d'une personne ayant mené une campagne électorale); si le traitement est nécessaire à des recherches scientifiques, etc.

Les données relatives aux suspicions, poursuites et condamnations peuvent être traitées par une autorité publique si cela est nécessaire à l'exercice de ses tâches; par un avocat pour la défense de ses clients; par quiconque pour la gestion de son propre contentieux; ou, si c'est nécessaire, à la réalisation de finalités fixées par la loi.

Pour toutes ces hypothèses, des garanties supplémentaires sont à respecter, notamment :

- 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 [44]. Cela n'oblige pas le responsable du traitement à désigner les personnes par leur nom, mais plutôt à établir des profils d'accès (p. ex., les inspecteurs sociaux, les membres d'une équipe éducative);
- les personnes traitant des données sensibles devront être tenues par une obligation de confidentialité qu'elle soit légale, statutaire ou contractuelle [45].

Comment identifier la personne légalement responsable du traitement ?

Il est primordial de pouvoir déterminer qui est le responsable du traitement, car c'est à lui qu'incombe l'obligation de respecter la plupart des obligations définies par la loi du 8 décembre 1992. Il convient de distinguer à cet égard deux hypothèses :

- Le traitement est prévu **dans un texte légal** qui désigne qui sera considéré comme le responsable du traitement [46].
- **Dans tous les autres cas :** le responsable du traitement est la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.

La qualité de responsable du traitement dépend donc d'une situation de fait : il convient pour chaque traitement de déterminer qui se charge ou a le pouvoir de décider des finalités du traitement ainsi que des moyens mis en œuvre pour le réaliser. Il peut s'agir de plusieurs personnes lorsqu'elles participent toutes à la détermination des finalités et des moyens de traitement. Dans ce cas elles sont coresponsables du traitement.

Il est à noter que la détermination de l'identité du responsable du traitement et de l'établissement dans le cadre duquel intervient le traitement jouent un rôle pour déterminer si c'est bien la loi belge qui est applicable. La loi du 8 décembre 1992 s'applique en effet lorsque le traitement

(42) *Loi du 8 décembre 1992, art. 6, 7 et 8.*
(43) *Loi du 8 décembre 1992, art. 6, 7 et 8.*
(44) *A.R. du 13 février 2001, art. 25,1.*
(45) *Loi du 8 décembre 1992, art. 8, § 3 et A.R. du 13 février 2001, art. 25, 3°.*
(46) *Loi du 8 décembre 1992, art. 1er, § 4.*

est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge ou en un lieu où la loi belge s'applique en vertu du droit international public [47].

Que doit-on faire avec les données recueillies ?

Veiller à la qualité des données

Les données que l'on traite doivent être exactes et, si c'est nécessaire, mises à jour. Le responsable du traitement doit prendre toutes les mesures raisonnables pour corriger ou effacer les données qui sont inexactes ou incomplètes.

Veiller à la confidentialité des données

Le responsable du traitement doit veiller à ce que les personnes travaillant sous son autorité n'aient accès et ne puissent utiliser que les données dont elles ont besoin pour exercer leurs fonctions. Il n'est pas question de permettre aux membres du personnel d'avoir accès à des données qui ne leur sont pas nécessaires [48].

Le responsable doit en outre mettre son personnel au courant des prescrits des dispositions légales en matière de protection des données [49]. Il doit expliquer les principes de protection qui doivent désormais être respectés. Cela peut, par exemple, être réalisé par des formations effectuées en interne ou par la mise à disposition d'un petit guide pratique, sur papier ou sur l'intranet, qui reprend les principes légaux à respecter.

Veiller à la sécurité des données

Le responsable du traitement est tenu de protéger les données 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 les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel [50].

Ces mesures de sécurité que doit prendre le responsable du traitement sont donc de deux ordres : des mesures organisationnelles (limiter le nombre de personnes ayant accès aux données, fermer les locaux où sont localisés les ordinateurs et les fichiers, etc.) et des mesures techniques (protéger les bases de données contre les virus (programme antivirus, *firewalls*), utiliser des droits d'accès - mots de passe et nom d'utilisateur, cryptage, protection des locaux contre les incendies, dégâts des eaux, etc.).

La loi du 8 décembre 1992 précise que ces mesures doivent assurer 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, d'autre part, de la nature des données à protéger et des risques potentiels. Plus les données en cause sont sensibles et les risques pour la personne concernée grands, plus importantes seront les précautions à prendre.

Prévoir certaines garanties en cas de sous-traitance

Le responsable du traitement peut confier l'exécution des opérations de traitement à un tiers sous-traitant. Le sous-traitant est donc 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.

On peut également citer l'exemple de la société informatique qui se charge du *back up* des données du responsable du traitement ou de la société de publipostage qui se charge de l'envoi de courrier sur la base d'une liste de destinataires établie par ses clients, ou encore lorsque l'on confie à des tiers certains services tels des *call centers*, des services informatiques ou *business process* (outsourcing) [51].

En revanche, les employés ne sont pas des sous-traitants de leur employeur [52].

Le responsable du traitement qui confie tout ou partie du traitement de données à caractère personnel à un sous-traitant doit s'assurer que celui-ci offre des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements. Il doit conclure avec ce dernier un contrat par écrit, sur support papier ou électronique, au sein duquel il est prévu que le sous-traitant veillera à appliquer ces mesures et qu'il n'agira que sur instruction du responsable du traitement et veillera à ce que son personnel respecte ce principe. Le contrat doit également fixer la responsabilité du sous-traitant vis-à-vis du responsable du traitement [53].

En cas de sous-traitance d'un traitement effectué sur des données sensibles, le responsable du traitement devra prévoir une obligation de confidentialité à charge du sous-traitant.

Effacer les données

Les données personnelles ne doivent pas être conservées sous une forme qui permette d'identifier les personnes plus longtemps qu'il n'est nécessaire par rapport à l'objectif poursuivi. Il convient alors de les effacer ou de les rendre anonymes.

---

(47) Loi du 8 décembre 1992, art. 3bis, 1°.

(48) Loi du 8 décembre 1992, art. 16, § 2, 2°.

(49) Loi du 8 décembre 1992, art. 16, § 2, 3°.

(50) Loi du 8 décembre 1992, art. 16, § 4.

(51) T. VAN OVERSTRAETEN, «La protection des données à caractère personnel : quelques réflexions de praticien», in Les 25 marchés émergents du droit, ss. dir. L. DU MARLIÈRE, Bruxelles, Bruylant, 2006, pp. 357-358.

(52) Cf. Chapitre III, infra.

(53) Loi du 8 décembre 1992, art.16, § 1.

Quels sont les droits des personnes concernées à prendre en compte par le responsable du traitement ?

Parallèlement aux conditions définies pour la mise en œuvre d'un traitement de données à caractère personnel, la loi du 8 décembre 1992 spécifie les droits dont bénéficient les personnes concernées. Elle reconnaît aux personnes dont les données font l'objet d'un traitement un droit d'accès aux données, un droit de rectification et un droit d'opposition au traitement pour des motifs sérieux et légitimes tenant à la situation particulière de la personne concernée [54].

Permettre un exercice effectif de ces droits implique que le responsable de traitement en tienne compte lors de l'organisation des traitements qu'il entend mettre en œuvre. Le responsable du traitement devra en effet répondre et donner à la suite des demandes qui lui sont adressées dans ce contexte dans le délai prescrit par la loi. Aussi, si les données traitées sont éparpillées au sein de différentes bases de données, il sera plus difficile de donner suite à une demande d'accès ou de s'assurer que les demandes de rectifications seront correctement exécutées pour toutes les données qui se trouvent traitées ci et là dans l'organisation concernée.

Outre le droit à l'information évoqué *supra* à propos du principe de transparence, le responsable du traitement doit veiller au respect des droits des personnes suivants :

Le droit à la curiosité

Toute personne a le droit d'interroger tout responsable du traitement pour savoir s'il détient ou non des données sur elle. Le responsable interrogé doit confirmer ou non s'il détient des données la concernant et, si c'est le cas, il doit préciser dans quel but il détient les données, de quelles catégories de données il s'agit et quels sont les destinataires de ces données [55].

Le droit d'accès direct

Toute personne a le droit de recevoir, sous une forme intelligible, une copie des données faisant l'objet d'un traitement, ainsi que toute information disponible sur l'origine des données [56]. Le droit de connaître la provenance des données utilisées est particulièrement important, car c'est souvent la question de la source des informations qui préoccupe les personnes concernées. Il arrive cependant que cette source ne soit plus disponible parce que, par exemple, le fichier a été constitué au moyen de différentes sources, avant l'entrée en vigueur de la loi en 1998, lorsque le responsable du traitement n'avait pas encore l'obligation de conserver cette source.

C'est la raison pour laquelle la loi parle de la communication de toute information «disponible» sur l'origine des données.

Le droit d'accès indirect

En deux circonstances, c'est un accès indirect de la personne concernée à ses données qui est prévu.

L'accès aux *données relatives à sa santé* peut s'effectuer soit directement par la personne sur qui portent les données, soit par l'intermédiaire d'un professionnel des soins de santé choisi par cette personne, si le responsable du traitement ou la personne elle-même sollicite l'intervention d'un intermédiaire [57].

Pour les *données traitées à des fins de sûreté de l'État, de sécurité publique, de défense nationale, de prévention ou de répression des infractions*, c'est également un accès indirect qui est mis en place [58]. Dans ces cas, il faut s'adresser à la Commission de la protection de la vie privée en apportant la preuve de son identité et en lui demandant d'effectuer la démarche d'accès. La Commission effectue les vérifications utiles, fait procéder aux modifications nécessaires et spécifie à l'intéressé qu'il a été procédé aux vérifications, sans pouvoir pour autant en révéler la teneur.

Le droit de rectification

Toute personne peut, sans frais, faire rectifier les données inexactes qui se rapportent à elle [59] et faire effacer ou interdire d'utilisation les données incomplètes, non pertinentes ou interdites [60].

Si des données inexactes, incomplètes, non pertinentes ou interdites ont été transmises à des tiers, le responsable doit, dans le mois, signaler les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées, à moins que cela ne s'avère impossible ou extrêmement difficile.

Le droit d'opposition

Toute personne a le droit de s'opposer à ce que les données la concernant fassent l'objet d'un traitement, mais elle doit invoquer des raisons sérieuses et légitimes [61].

Il existe toutefois *des limites du droit d'opposition :* le droit d'opposition n'est pas admis pour les traitements nécessaires à la conclusion ou à l'exécution d'un contrat; les personnes concernées ne peuvent pas non plus s'opposer au traitement de leurs données imposé par une obligation légale ou réglementaire.

Lorsque les données sont collectées *à des fins de marketing direct* (pour des démarches publicitaires), la personne concernée peut s'opposer gratuitement et sans aucune justification au traitement de ses données.

(54) Loi du 8 décembre 1992, art.10 et 12.
(55) Loi du 8 décembre 1992, art. 10, § 1er, a).
(56) Loi du 8 décembre 1992, art. 10, § 1er, b).
(57) Loi du 8 décembre 1992, art. 10, § 2.
(58) Loi du 8 décembre 1992, art. 13.
(59) Loi du 8 décembre 1992, art. 12, a).
(60) Loi du 8 décembre 1992, art. 12, § 1er, al.5.
(61) Loi du 8 décembre 1992, art. 12, § 1er, al.2.

Le droit de ne pas être soumis à une décision automatisée

Il n'est pas souhaitable qu'une décision qui s'impose à un être humain dépende des seules conclusions d'une machine. Aussi, la loi interdit qu'une décision affectant une personne de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité (p. ex., pour l'octroi d'un avantage, sur la base de critères prédéterminés dans une application informatique) [62]. 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 garantissant la sauvegarde des intérêts de l'intéressé. À tout le moins, celui-ci doit avoir le droit de faire valoir *utilement* son point de vue.

Sanctions

D'un point de vue de la responsabilité civile, l'article 15 de la loi du 8 décembre 1992 prévoit que c'est le responsable du traitement qui sera considéré comme responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la loi et qu'il n'est exonéré de cette responsabilité que s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.

Les articles 38 et 39 de loi du 8 décembre 1992 érigent en infractions pénales la violation de la plupart des dispositions de la loi.

*(62) Loi du 8 décembre 1992, art. 12*bis.