BeLHIS

BELGIAN LONGITUDINAL HEALTH INFORMATION SYSTEM

RAPPORT COMPLET

Vie privée et intégration des données de santé

Privacy en integratie van gezondheidsgegevens

BELGIAN LONGITUDINAL HEALTH INFORMATION SYSTEM

COMPLÉTER LE SYSTÈME D'INFORMATION SANITAIRE AU MOYEN DE DONNÉES PROVENANT D'UNE PERSPECTIVE LONGITUDINALE DYNAMIQUE

TOEVOEGEN VAN EEN LONGITUDINALE COMPONENT AAN HET GEZONDHEIDS-INFORMATIESYSTEEM

RAPPORT COMPLET

Vie privée et intégration des données de santé

Privacy en integratie van gezondheidsgegevens

AGORA Contrat n° AG/JJ/139

CE RAPPORT PEUT ÊTRE RÉFÉRENCÉ
DE LA MANIÈRE SUIVANTE:

Cols F, D'hoore W, Doumont D, Coppieters Y, Deboosere P, Ingenbleek A, Lammens L, Levêque A,
Vie privée et intégration des données de santé.
Rapport complet, Projet BeLHIS, AGORA AG/JJ/139, Bruxelles, 2010.

Version définitive : Septembre 2008

Une synthèse de ce document est disponible sous la référence :
Doumont D, Cols F, D'hoore W, Coppieters Y, Deboosere P, Ingenbleek A, Lammens L, Levêque A,
Vie privée et intégration des données de santé.
Working paper N° 3, Projet BeLHIS, AGORA AG/JJ/139, Bruxelles, 2010.

Table des matières

Table des matières 3
PREMIERE PARTIE 7
LE CADRE LEGAL BELGE EN MATIERE DE PROTECTION DE LA VIE PRIVEE LORS DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL 7
Introduction 8
Chapitre I^er. – A qui et à quoi s'applique la loi? 9
Section I^ère. – Explication et définition des concepts-clés de la loi sur la protection de la vie privée 9
§ 1^er. – Données à caractère personnel 9
A. Différence entre donnée et information 9
B. L'information doit concerner une personne physique 10
C. La personne doit être identifiée ou identifiable 11
D. Application à une perspective longitudinale 12
§ 2. – La notion de traitement 12
§ 3. – Distinction entre dossier et fichier 12
§ 4. – Le responsable du traitement 13
§ 5. – Le sous-traitant 14
§ 6. – Le tiers et le destinataire 15
§ 7. – La notion de consentement de la personne concernée 16
Section II. – Le champ d'application matériel et personnel 17
§ 1^er. – Le champ d'application matériel 17
§ 2. - Le champ d'application personnel 18
§ 3. – Les exceptions 19
A. Traitement effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques 19
B. Traitement effectué aux seules fins de journalisme ou d'expression artistique ou littéraire 19
C. Exceptions en matière de Sûreté de l'Etat, de services de renseignements et de police 20
D. Traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques 20
Section III. – Le champ d'application territorial 26
Section IV. – Le champ d'application temporel 28
Chapitre II. – Comment vérifier le respect de la protection de la vie privée? 28
Section I^ère. – Les conditions de licéité du traitement de données à caractère personnel 28
§ 1^er. – Les conditions générales 28
A. Les conditions relatives à la qualité du traitement des données (art. 4) 29
B. Les conditions de légitimité du traitement de données à caractère personnel 31
§ 2. – Le traitement de catégories particulières de données à caractère personnel 33
§ 3. – Le traitement des données dites sensibles 35

A. Que recouvre la notion de "données sensibles"? 35
B. Le régime juridique: interdiction de principe assortie d'exceptions 36
§ 4. – Le traitement des données relatives à la santé 40
A. Que recouvre la notion de données relatives à la santé? 41
B. Le régime juridique: interdiction de principe assortie d'exceptions 41
C. Les garanties supplémentaires 46
§ 5. – Le traitement des données judiciaires 48
Section II. – Les droits de la personne concernée et les obligations du responsable du traitement 49
§ 1er. – Le droit à la protection des libertés et droits fondamentaux, notamment à la protection de la vie privée 49
§ 2. – Le droit à l'information 50
A. Obtention des données auprès de la personne concernée 50
B. Obtention auprès de tiers 51
C. Les modalités de l'information 52
D. Les exceptions à l'obligation d'information 53
§ 3. – Le droit d'accès 56
A. Les conditions du droit d'accès 56
B. L'information qui doit et peut être communiquée 57
C. Les modalités de la réponse du responsable du traitement à la demande de la personne concernée 58
D. Les exceptions et le droit d'accès indirect 58
§ 4. – Le droit d'opposition 59
A. Le droit général d'opposition 59
B. Le droit d'opposition en matière de marketing direct 60
C. Les conséquences de l'exercice du droit d'opposition 62
§ 5. – Le droit de rectification 62
§ 6. – Le droit de ne pas être soumis à des décisions individuelles automatiques 63
§ 7. – Le droit d'introduire un recours en justice 63
Section III. – Les mécanismes de contrôle 64
§ 1er. – Le contrôle interne: les obligations en matière de sécurité et de confidentialité du traitement 64
A. Obligations en matière de sécurité des données à caractère personnel 64
B. Les obligations techniques et organisationnelles concrètes 67
C. Relation avec le sous-traitant 68
D. La confidentialité du traitement 69
§ 2. – Le contrôle externe: la déclaration auprès de la Commission de la protection de la vie privée et les compétences de celle-ci 69
A. La déclaration 70
B. Le registre public 75
C. Les compétences de la Commission 76
D. Les règles de composition et de fonctionnement de la Commission 77
Conclusion 79
Bibliographie 80
DEUXIEME PARTIE 82
DEUX SUJETS D'ACTUALITE 82

Chapitre I[er]. – eHealth, la plate-forme électronique d'échange des données relatives à la santé 83
Section I[ère]. – Les origines: la plate-forme Be-Health *83*
§ 1[er]. – De l'accord de principe à la création de la plate-forme Be-Health 83
§ 2. – Fonctionnement et applications de la plate-forme Be-Health 85
A. Accès limité et respect de la vie privée 85
B. L'application Registre du Cancer 87
C. Autres applications 87
Section II. – Le projet eHealth *88*
§ 1[er]. – Un projet prioritaire 88
§ 2. – Présentation du contenu du projet de loi 89
A. Une institution publique dotée de la personnalité juridique, au sein de la Banque Carrefour de la Sécurité Sociale 89
B. Les objectifs de la plate-forme eHealth 90
C. Les missions de la plate-forme eHealth 91
D. Les droits et obligations de la plate-forme eHealth 93
E. La gestion de la plate-forme eHealth 98
F. Le Comité de concertation des utilisateurs de la plate-forme eHealth 99
G. L'autorisation d'association 100
§ 3. – Les recommandations de la Commission de la protection de la vie privée (CPVP) et du Conseil d'Etat 101
A. L'avis de la Commission de la protection de la vie privée 101
B. L'avis du Conseil d'Etat 105
§ 4. – Les critiques adressées par les associations de médecins 107
A. La réaction de l'Association belge des syndicats médicaux (ABSyM) 107
B. Réaction du Forum des associations de généralistes (FAG) 111
C. Réaction du Conseil national de l'Ordre des Médecins (CNOM) 112
D. Les critiques adressées quant à la méthode 112
E. Les critiques adressées du point de vue juridique 114
§ 5. – Les justifications avancées par les créateurs du projet et leurs réponses aux critiques adressées à celui-ci 116
A. Caractère facultatif de la plate-forme eHealth 116
B. Respect et soutien des initiatives locales, et absence de tout monopole 117
C. Sécurité et protection de la vie privée 118
D. Relation avec la BCSS 120
E. Représentation de tous les acteurs des soins de santé, et volonté de les impliquer 121
F. Des services à valeur ajoutée 122
G. Réputation internationale et européenne de la Belgique 122
§ 6. – Les amendements et garde-fous apportés au projet 123
A. La définition des données à caractère personnel relatives à la santé 123
B. La gratuité des services de base 123
C. Les garanties supplémentaires entourant la mission d'organisme intermédiaire de la plate-forme eHealth 124
D. Les précisions au sujet de l'autorisation de la section santé du comité sectoriel de la sécurité sociale et de la santé, et la création de cette dernière 124

E. La composition du Comité de gestion, le contrôle de la plate-forme eHealth et le Comité de concertation 125
F. L'évaluation de la loi deux ans après son entrée en vigueur 126
Section III. – Conclusion 126
Chapitre II. – L'utilisation du numéro du Registre national des personnes physiques ... 127
Section Ière. – La loi du 8 août 1983 organisant un Registre national des personnes physiques 127
§ 1er. – Accès aux informations enregistrées et conservées par le Registre national 127
§ 2. – Autorisation d'utilisation du numéro d'identification du Registre national . 128
§ 3. – Le Comité sectoriel du Registre national 129
Section II. – Jurisprudence de la Commission de la protection de la vie privée relative au numéro d'identification unique en santé 129
§ 1er. – De l'utilisation d'un numéro d'identification spécifique au secteur de la santé… 129
§ 2. – … à l'utilisation du numéro d'identification du registre national 130
Section III. – Le cas de la Fondation Registre du Cancer 134
§ 1er. – L'accès au registre national et l'usage du numéro d'identification du registre national par l'œuvre belge du cancer 134
§ 2. – Le système du Registre National du Cancer : deux clés de codage 134
§ 3. – Le système actuel de la Fondation Registre du Cancer 135
Bibliographie 137

PREMIERE PARTIE

LE CADRE LEGAL BELGE EN MATIERE DE PROTECTION DE LA VIE PRIVEE LORS DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Introduction

De nombreuses activités menées dans le cadre de ce que l'on appelle la santé publique touchent à la vie privée des individus, étant susceptibles d'y porter atteinte dans certaines circonstances. S'il est important de protéger cette vie privée afin d'empêcher les abus dont elle pourrait être la victime, il convient également d'offrir la possibilité de mener des études et recherches permettant d'améliorer la santé publique de notre pays. En effet, un régime trop strict qui interdirait toute recherche impliquant certains aspects de la vie privée des individus, empêcherait de mener d'efficaces politiques de promotion de la santé, de connaître les problèmes existants et d'y apporter des solutions. Afin de garantir la protection de ces deux intérêts, l'un individuel et l'autre sociétal ou collectif, et de maintenir un équilibre entre ceux-ci, la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel fut adoptée en Belgique le 8 décembre 1992[1]. Cette législation vise à réglementer les traitements de données à caractère personnel, sans toutefois les interdire purement et simplement. Elle consiste donc à encadrer cette pratique de certaines limites à ne pas dépasser, afin de garantir le respect d'un certain nombre de valeurs estimées essentielles à notre société.

Afin de savoir ce qu'il est possible de faire en matière de santé publique, en Belgique et conformément à la législation actuelle, il importe de se poser plusieurs questions. Tout d'abord, à qui et à quoi s'applique la loi? En effet, cette loi ne vise qu'un aspect particulier de la vie privée – à savoir les données à caractère personnel – et ne s'applique qu'à certains acteurs, certains traitements, etc. Les interdictions ou limitations de principe sont bien souvent assorties d'exceptions, qu'il convient de bien circonscrire afin de savoir si la loi est applicable ou non au cas d'espèce dont il s'agit. Dans un deuxième temps, il convient de se demander comment la protection et le respect de la vie privée sont garantis et assurés, dans les cas auxquels la loi s'applique. Quels sont les différents droits dont jouissent les acteurs concernés, et les obligations auxquelles ils sont soumis? Quels mécanismes de contrôle sont mis en place afin de vérifier que la loi soit correctement appliquée et respectée?

Nous tenterons de répondre à ces différentes questions, à la lumière de la législation actuelle et des travaux parlementaires y relatifs, ainsi que des éclairages que peuvent apporter la doctrine et la jurisprudence.

Notons que la loi belge a été modifiée en 1998, suite à la transposition de la directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[2]. La Belgique a donc dû adapter ses concepts, définitions et réglementations afin de se conformer à la législation européenne. Nous nous baserons ici sur la version coordonnée de la loi belge, c'est-à-dire la version incluant toutes les modifications survenues depuis l'existence de la loi, même si de temps à autres une allusion à l'ancienne version sera faite lorsqu'elle s'avèrera utile et intéressante.

---

[1] L. 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, http://www.moniteur.be.

[2] Directive européenne 95/46/C.E. 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.,* L 281/31, 23 nov. 1995, http://www.eur-lex.europa.eu.

Chapitre I[er]. – A qui et à quoi s'applique la loi?

Avant de savoir ce à quoi la loi nous oblige, il convient de s'assurer qu'elle nous soit applicable. Cela revient à examiner quel est le champ d'application de la loi, ce qui nécessite d'analyser non seulement les dispositions de la loi relatives au champ d'application lui-même, mais également et avant tout celles qui définissent les concepts-clés de la législation.

Section I[ère]. – Explication et définition des concepts-clés de la loi sur la protection de la vie privée

Contrairement à ce que l'on pourrait penser, la question de la définition des concepts empruntés par la loi sur la protection de la vie privée revêt bien plus qu'un intérêt purement théorique, conceptuel et intellectuel. En effet, le champ d'application de la loi lui-même dépend du caractère plus ou moins large ou étroit attribué aux concepts qui en font partie. Une bonne délimitation de ceux-ci contribue à comprendre et à déterminer précisément les situations visées par la loi, ainsi que les conséquences que cela implique. Cet exercice n'est donc nullement dépourvu de toute pertinence pratique, mais porte au contraire une utilité concrète, et mérite que l'on y prête attention.

§ 1[er]. – Données à caractère personnel

La loi du 8 décembre 1992 ne vise à protéger qu'un aspect particulier de la vie privée, à savoir les données à caractère personnel des personnes physiques qui font l'objet d'un traitement. La première question à se poser afin de savoir si la loi est applicable en l'espèce, consistera à savoir si nous sommes en présence de données à caractère personnel. Il importe donc de bien délimiter ce que recouvre cette notion, que la loi définit en son article 1[er], § 1[er], comme étant "toute information concernant une personne physique identifiée ou identifiable". Plusieurs éléments de cette définition légale peuvent prêter à confusion, d'où l'intérêt de les envisager un à un pour en préciser le contenu.

A. Différence entre donnée et information

Il convient tout d'abord de clarifier le concept d'information, sa signification différant de celle du concept de donnée. Si une donnée vise toute chose par laquelle un être humain peut être déterminé, l'information se réfère à la naissance ou à l'augmentation d'une connaissance à propos de cet être humain, tout comme à la disparition d'une incertitude à son sujet. Ainsi, l'information se caractérise par le fait qu'une donnée est portée à notre connaissance, créant ou augmentant ce que l'on sait au sujet de la personne que la donnée concerne. Une donnée pouvant nous parvenir par un support écrit,

oralement ou même par une sensation ou une perception (d'un bruit, d'une odeur ou d'une image), l'information n'est soumise à aucune exigence de forme, ni de structure[3].

B. L'information doit concerner une personne physique

La loi précise qu'elle ne concerne que les personnes physiques, excluant de la sorte les **personnes morales** de son champ d'application. Ainsi, le traitement de données relatives à une société n'est pas protégé par la loi. Toutefois, si ce traitement implique celui de données personnelles des personnes physiques membres de cette société, la loi s'appliquera.

L'on pourrait croire que l'exigence de l'existence d'une personne physique exclue également les données relatives aux personnes non encore nées, à savoir les **embryons**. Il convient cependant de formuler deux remarques à ce sujet. Tout d'abord, ce genre de données inclut régulièrement des données relatives aux parents de l'enfant à naître. Ces données concernant des personnes physiques vivantes, la loi leur est applicable. S'agissant des données relatives au fœtus lui-même, celui-ci n'ayant pas la personnalité juridique, elles ne peuvent être qualifiées de données à caractère personnel. La doctrine plaide toutefois en faveur d'une protection de ces données de manière comparable, sinon égale, à la protection accordée aux données à caractère personnel. D'ailleurs, la Recommandation R (97) 5 du Conseil de l'Europe en matière de données médicales déclare, en son article 4.5, que les données relatives aux enfants non nés doivent être considérées comme des données à caractère personnel, et recevoir une protection semblable à celle dont jouissent les données médicales de mineurs[4].

S'agissant des données relatives aux **défunts**, il convient de distinguer deux situations. Dans certains cas, ces données sont susceptibles de fournir des informations sur des parents vivants, ce qui implique qu'il faille les considérer comme des données à caractère personnel. Pour ce qui est des données strictement relatives au défunt, la personnalité juridique s'éteignant avec la mort, certains auteurs considèrent que ces données perdent toute protection après la mort. D'autres, au contraire, estiment que le fait que le défunt ne jouisse plus des droits que la loi sur la protection de la vie privée lui reconnait, n'implique pas que les dispositions de cette loi cessent de s'appliquer une fois que la personne concernée est décédée. Autrement dit, la collecte, le traitement et l'usage de ces données ne peut être rendu totalement libre par le simple fait de la mort[5].

Il importe enfin de signaler que le lien qui unit l'information et la personne physique ne doit pas nécessairement être direct: il suffit que l'information se rapporte à une personne physique[6].

---

[3] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 23.
[4] Recommandation n° R (97) 5F du 13 février 1997 du Comité des Ministres du Conseil de l'Europe aux Etats membres relative à la protection des données médicales, p. 28, http://www.coe.int; D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 25.
[5] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 26-27.
[6] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 27.

C. La personne doit être identifiée ou identifiable

Pour être qualifiée de donnée à caractère personnel, il ne suffit pas que l'information se rapporte à une personne physique, il faut en outre qu'elle permettre d'identifier la personne concernée. A ce sujet, il convient de distinguer, selon D. De Bot[7], les données identifiantes directes, des données identifiantes indirectes. Si les premières sont en soi suffisantes pour immédiatement identifier la personne concernée (telles que le nom et le prénom, ou le numéro d'identification du registre national), les autres se réfèrent aux éléments caractérisant une personne et susceptibles de permettre son identification (par exemple, un numéro de téléphone, de plaque d'immatriculation de véhicule, ou encore le numéro de carte d'identité). Cette distinction n'est que conceptuelle, le régime juridique étant le même dans les deux cas: la loi s'applique invariablement, que la personne soit identifiée ou identifiable, dès que la possibilité existe de pouvoir identifier la personne concernée. En effet, les travaux parlementaires précisent qu'"une information relative à une personne est donc considérée comme donnée à caractère personnel tant que quelqu'un est encore en mesure, par quelque moyen qui puisse raisonnablement être mis en œuvre, de déterminer à quel individu se rapporte cette information. Sont donc également considérées comme données à caractère personnel les informations codées pour lesquelles le responsable du traitement lui-même ne peut vérifier à quelle personne elles se rapportent, parce qu'il ne possède pas les clefs nécessaires à son identification, lorsque l'identification peut encore être effectuée par une autre personne"[8]. Ainsi, "dès lors qu'il existe un moyen raisonnable d'identifier les personnes concernées, soit dans le chef du responsable du traitement, soit même par un tiers, il s'agit d'une donnée à caractère personnel dont le traitement est susceptible d'être réglementé par la loi"[9]. C'est donc *in abstracto* qu'il convient de considérer la possibilité d'identifier la personne concernée, et non au regard des moyens techniques dont dispose le responsable du traitement.

Il résulte de cette analyse que seules sont exclues du champ d'application de la loi les données anonymes, à savoir celles qui ne permettent pas d'identifier la personne concernée. Ainsi par exemple, un système de codage irréversible de certaines données personnelles, aboutissant à un certain nombre de chiffres exempts de toute information relative à la personne concernée, permettrait d'opérer un traitement sans être soumis à la loi. Par contre, le traitement de données codées n'est pas nécessairement exclu du champ d'application de la loi, étant donné que l'identification des personnes concernées demeure possible. En effet, si le responsable du traitement n'est pas toujours en possession de la clé permettant de décoder les données, l'organisme qui a procédé au codage des données reste capable de retourner à l'information identifiante, et cela suffit pour considérer les données codées comme étant à caractère personnel.

---

[7] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 27-29.
[8] Exposé des motifs, p. 12.
[9] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 378.

D. Application à une perspective longitudinale

Dans le cas d'une étude longitudinale, les données seront nécessairement à caractère personnel, puisque les personnes doivent être identifiables, le caractère longitudinal d'une recherche impliquant le suivi des mêmes personnes dans le temps. Le codage des données n'entre pas en ligne de compte, étant donné que la seule possibilité d'identifier les personnes concernées, ce que l'organisme chargé du codage des données reste en mesure de faire, suffit à considérer les données comme étant à caractère personnel.

§ 2. – La notion de traitement

La notion de traitement présente moins de difficultés que celle de données à caractère personnel. La loi, en son article 1er, § 2, la définit de manière très large, se référant à toute opération ou ensemble d'opérations, effectuées ou non à l'aide de procédés automatisés – notons qu'avant la réforme de 1998, la loi opérait une distinction selon que le traitement était réalisé à l'aide de moyens automatisés ou non. Ainsi, dès la simple collecte, toute opération, même isolée, sur des données consiste en un traitement. Celui-ci se réfère donc au processus, constitué d'une ou plusieurs opérations. Par "ensemble d'opérations", il convient d'entendre toute concentration d'opérations qui peut être considérée comme un tout[10]. S'agissant d'opérations uniques ou isolées, afin de pouvoir être considérées comme traitement au sens de la loi, elles doivent conférer, d'une manière ou d'une autre, une autorité ou un contrôle sur les données à caractère personnel[11].

La loi énonce, de manière non limitative, un certain nombre d'opérations à considérer comme traitement, à savoir 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. Cette liste n'est qu'exemplative, comme l'indiquent les termes "telles que" empruntés par la loi, ne limitant d'aucune manière l'application de la loi aux seules opérations énumérées.

§ 3. – Distinction entre dossier et fichier

La loi s'appliquant aux fichiers, et non aux dossiers non automatisés, il importe de bien différencier ces deux concepts. Ceux-ci concernent les cas de traitements manuels, c'est-à-dire non-automatisés. La loi définit le ficher comme étant "tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que

[10] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 37.
[11] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 41.

cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique" (art. 1er, § 3). Ainsi, afin de déterminer si un ensemble de données à caractère personnel est un fichier, il convient de vérifier le respect de deux conditions: il faut que les données soient structurées selon des critères relatifs aux personnes, et que ces critères personnels permettent un accès facile aux données à caractère personnel[12]. Autrement dit, "la structure des données à caractère personnel doit permettre leur accessibilité selon des critères déterminés"[13].

Sont donc non pertinentes en la matière les considérations d'ordre temporel, l'existence d'un fichier étant indépendante de la conservation ou non des données.

Notons que l'ancienne version de la loi prévoyait deux autres exigences quant à l'existence d'un fichier, à savoir une structure logique, permettant une consultation systématique – ces deux conditions peuvent être rassemblées en un seul "critère d'organisation visant la consultation systématique"[14]. Elle exigeait en outre que l'ensemble de données personnelles ait un caractère durable, c'est-à-dire que les données soient conservées durant un certain temps.

§ 4. – Le responsable du traitement

L'identification précise de la personne qui peut être qualifiée de "responsable du traitement" relève d'une grande importance, celui-ci étant le destinataire de la plupart des obligations prévues par la loi, ainsi que des sanctions qui s'appliqueront en cas de non-respect de ces obligations.

La loi établit comme critère fonctionnel la compétence de prendre les décisions relatives au traitement concerné. Ce critère se décline en deux conditions cumulatives, à savoir le pouvoir de déterminer à la fois les finalités et les moyens du traitement[15]. Le responsable du traitement est donc celui qui est en mesure de décider des finalités et des moyens du traitement. Diverses situations particulières méritent toutefois d'être envisagées.

Tout d'abord, la possibilité d'une prise de décision conjointe en la matière est légalement envisagée, ce qui implique dans ce cas que plusieurs personnes seront identifiées comme responsables du même traitement[16]. Cela ne signifie toutefois pas nécessairement que les différents responsables seront juridiquement tenus à une responsabilité commune. En effet, si différentes personnes ou entreprises traitent des

---

[12] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 328.

[13] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 379.

[14] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 328.

[15] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 45.

[16] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 379.

données issues d'une même banque de données, déterminant chacune les finalités et moyens du ou des traitement(s) qu'elles opèrent, chacune sera responsable pour son ou ses traitement(s)[17]. A ce sujet, notons que dans le cas d'organisations ou d'entreprises, le fait que la décision soit prise par le conseil d'administration ou par un autre organe de la sorte, ne rend pas les membres de cet organe personnellement responsables du traitement. C'est l'organisation ou l'entreprise elle-même qui sera identifiée comme responsable. Il n'en va pas de même si le traitement est effectué par une personne physique[18].

De manière semblable, la responsabilité pour un traitement peut varier selon les données qui sont traitées, comme ce peut être le cas lors de traitements en matière de services de télécommunications et des nouvelles technologies – internet, par exemple –, dans lesquels interviennent de nombreux acteurs[19].

Selon D. De Bot, si la personne investie du pouvoir de décision quant aux finalités du traitement n'est pas la même que celle qui décide des moyens, il convient de donner la priorité à celle qui détermine les finalités, au motif que cette solution est celle qui s'adapte le mieux à la pratique[20].

Un autre cas particulier concerne les traitements de données au sein d'un même groupe, en augmentation ces derniers temps suite à la concentration croissante des entreprises qui marque la vie économique. Le responsable du traitement est la personne morale à qui revient la compétence du traitement opérationnel, sans que le pouvoir de fait ou l'influence d'autres personnes morales appartenant au groupe n'entre en ligne de compte dans l'identification du responsable du traitement[21]. Différents scénarios sont toutefois possibles, comme celui qui consisterait en l'attribution de la compétence de décider des finalités et des moyens du traitement à une personne morale déterminée, dans les statuts ou via un accord entre les personnes morales concernées.

S'agissant des traitements dont les finalités et les moyens sont déterminés par ou en vertu de la loi, le responsable du traitement sera la personne que cette même loi désigne, et ce afin d'éviter que le législateur lui-même puisse être considéré comme responsable du traitement en pareil cas[22] (art. 1er, § 4, al. 2).

Enfin, notons qu'un responsable de traitement établi à l'étranger en dehors du territoire de l'Union européenne est tenu de désigner un représentant en Belgique (art. 3*bis,* al.2).

§ 5. – Le sous-traitant

Le sous-traitant est la personne qui traite les données pour le compte du responsable du traitement (art. 1er, § 5). Il se distingue, et la loi le précise au sein même de la définition de la notion de sous-traitant, du préposé ou du fonctionnaire, ces derniers traitant les données sous l'autorité directe du responsable du traitement. La différence réside donc dans le caractère externe du sous-traitant, se situant en dehors de l'entreprise

[17] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 47.
[18] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 46.
[19] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 46-47.
[20] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 46.
[21] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 48.
[22] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 49.

ou de l'organisation du responsable du traitement, et n'agissant pas sous son autorité directe[23]. Ainsi par exemple, seront considérés comme sous-traitants au sens de la loi, le prestataire informatique qui gère le traitement, l'entreprise de marketing direct qui met à jour les données de ses clients, ou encore le secrétariat social qui gère le paiement des salaires pour une PME[24].

Notons que les relations entre le responsable du traitement et le sous-traitant sont réglées par contrat, la loi imposant certains éléments devant y figurer.

§ 6. – Le tiers et le destinataire

La notion de tiers est relativement facile à circonscrire, étant donné que la loi la définit négativement. Il s'agit de "toute autre personne que le responsable du traitement, le sous-traitant et les personnes qui traitent les données sous leur autorité directe"[25] (art. 1er, § 6). Il s'agit donc d'une personne totalement indépendante du responsable, qui n'appartient pas à l'organisation ou à l'entreprise de celui-ci, et qui est "indépendant de la manière selon laquelle le responsable du traitement a été désigné"[26].

Par "destinataire", la loi vise toute personne à qui sont communiquées des données (art. 1er, § 7). Il importe de préciser la portée de ce concept par rapport aux autres personnes intervenant dans le traitement de données. Si tout tiers à qui sont communiquées des données est un destinataire, tout destinataire n'est pas un tiers. La loi l'indique d'ailleurs expressément au sein de la définition de la notion de destinataire. Ainsi, peuvent également être destinataires des personnes ou services qui font partie de l'organisation ou de l'entreprise du responsable du traitement, à savoir par exemple, les membres du personnel d'autres services comme la section marketing. Ces destinataires peuvent être qualifiés de destinataires internes. A l'inverse, les destinataires externes visent les sous-traitants, qui sont toujours à la fois destinataires[27].

Enfin, la loi précise elle-même que "les instances administratives ou judiciaires qui sont susceptibles de recevoir communication de données dans le cadre d'une enquête particulière ne sont toutefois pas considérées comme des destinataires". Cette disposition vise par exemple les situations d'inspections fiscales ou sociales, ou les enquêtes judiciaires.

---

[23] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 52.
[24] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 379.
[25] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 379.
[26] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 55.
[27] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 56-57.

§ 7. – La notion de consentement de la personne concernée

Bien qu'elle n'intervienne pas dans la question du champ d'application de la loi, la dernière définition inscrite dans la loi du 8 décembre 1992 – et qui n'est pas sans importance, loin de là – vise la notion de consentement de la personne concernée, ce par quoi il convient d'entendre "toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement" (art. 1er, § 8). La loi énonce, par cette définition, cinq conditions à respecter pour pouvoir parler de véritable consentement de la personne concernée.

Tout d'abord, cette manifestation de volonté doit émaner de la personne concernée elle-même, ou de son représentant légal – lorsque la personne concernée est mineure, ou placée sous statut d'administration provisoire. Selon D. De Bot, cette précision implique que la volonté soit extériorisée, que ce soit de manière explicite ou implicite[28]. L'expression de volonté explicite résultera d'un acte clair spécialement exécuté pour exprimer la volonté; tandis que l'expression implicite peut être déduite, d'après les circonstances propres au cas d'espèce, d'un acte contenant une autre intention que celle d'exprimer la volonté, ou d'une abstention d'agir. Précisons que la loi vise toute manifestation de volonté, sans requérir d'écrit. Il peut donc être consenti au traitement de ses données à caractère personnel oralement.

La seconde condition exige que la manifestation de volonté soit libre, c'est-à-dire exempte de toute pression, menace ou violence destinée à forcer la personne concernée à consentir. Selon divers auteurs, cette exigence semble dans bien des cas être illusoire en pratique, étant donné que "la pression économique consistant dans le risque de se voir refuser un produit ou un service considérés à tort ou à raison comme essentiels par la personne concernée l'amènera bien souvent à donner son consentement sans aucun esprit critique"[29]. Il est donc recommandé au responsable de traitement, en cas de consentement par signature d'un document d'affiliation, de bien veiller à ce que les relations de force soient équilibrées, et que les traitements auxquels il est consenti par la signature de ce document soient décrits de manière suffisamment claire[30].

Le consentement doit en outre être spécifique, ce qui signifie qu'il ne peut avoir un objet général, mais doit porter sur un ou plusieurs traitements clairement définis. Il doit donc s'agir d'un traitement bien déterminé, réalisé par un responsable bien déterminé, et pour des finalités elles aussi bien déterminées.

La loi exige également que le consentement soit informé, imposant de la sorte au responsable d'informer dûment la personne concernée à propos des risques et avantages qu'entraîne sa participation au traitement. Toute l'information nécessaire à cette évaluation des risques du traitement doit donc être transmise à la personne concernée, et ce de manière compréhensible. Le respect de cette condition doit être apprécié selon les

---

[28] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 59.
[29] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 380. Voy. aussi D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 59.
[30] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 60.

circonstances du cas d'espèce[31]. L'article 9 de la loi précise plus en détail les contours de ce droit à l'information auquel peut prétendre la personne concernée, et dont le corolaire consiste en une obligation d'information dans le chef du responsable du traitement.

Enfin, une dernière condition concerne le sujet de la manifestation de volonté, à savoir l'acceptation par la personne concernée du traitement de ses données à caractère personnel.

Notons que ce consentement peut être retiré à tout moment, sans que ce retrait ne puisse pour autant agir de manière rétroactive. Cela signifie que les traitements effectués avant le retrait, et reposant sur un consentement répondant aux conditions légales, ne peuvent être annulés ni contestés sur base de ce retrait de consentement. Par contre, les traitements postérieurs à ce retrait ne pourront être menés.

Section II. – Le champ d'application matériel et personnel

Nous traiterons de ces deux aspects du champ d'application de la loi au sein d'une même section, les exceptions mentionnées par la loi touchant à chacun d'eux. En effet, certaines exceptions se justifient par l'objet spécifique du traitement, d'autres étant liées à la qualité du responsable du traitement.

§ 1er. – Le champ d'application matériel

Juridiquement, le champ d'application matériel vise à déterminer les situations de fait auxquelles la loi s'applique. Selon l'article 3, § 1er, la loi s'applique "à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier".

S'agissant des traitements automatisés, aucune condition supplémentaire n'est nécessaire à l'application de la loi: il suffit que tout ou partie du traitement soit réalisé(e) à l'aide de moyens automatisés. Selon D. De Bot, cela signifie que les données, ou du moins une partie des données, soient disponibles sur un support accessible automatiquement, à savoir non seulement un ordinateur, mais également toute technique par laquelle une ou plusieurs opérations peuvent être effectuées sans intervention directe de la main humaine[32]. Sont ainsi exclus les fax et photocopieuses, ces techniques ne pouvant par elles-mêmes effectuer aucune opération sans intervention humaine. Par contre, toutes les nouvelles technologies de l'information, telles que l'informatique, la télématique ou les réseaux de télécommunication, seront considérées comme traitements automatisés.

Quant aux traitements non-automatisés, ils ne tomberont sous le coup de la loi que si les données à caractère personnel sont contenues dans un fichier, ou du moins appelées à y figurer. La simple intention, dans le chef du responsable du traitement, d'enregistrer les données dans un fichier est donc suffisante. Il convient d'être attentif à ne pas

[31] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 61.
[32] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 64.

commettre une erreur qui, selon D. De Bot, est fréquemment commise. Si les données ne font partie que d'un dossier, et non d'un fichier, l'intention de traiter ultérieurement ces données à l'aide de moyens automatisés n'entre pas en ligne de compte: l'intention n'a d'intérêt que lorsqu'il s'agit de traitements non-automatisés. La loi ne s'applique donc pas aux données contenues dans un dossier, même s'il est prouvé qu'elles seront ultérieurement traitées de manière automatisée[33].

Nous pouvons dès lors proposer cette grille de raisonnement, élaborée par D. De Bot[34], et visant à déterminer si la loi est ou non applicable à un traitement.

- S'agit-il de données à caractère personnel?
  - Si non, la loi ne s'applique pas.
  - Si oui, se pose la question suivante:
- S'agit-il d'un traitement au sens de la loi? Il convient de vérifier, entre autres, que le responsable du traitement jouisse d'une autorité matérielle sur les données.
  - Si non, la loi ne s'applique pas.
  - Si oui, se pose la question suivante:
- Le traitement est-il automatisé?
  - Si oui, la loi s'applique.
  - Si non, se pose la question suivante:
- S'agit-il d'un fichier, au sens de la loi, c'est-à-dire selon le double critère de la structure facilitant l'accès aux données selon des critères déterminés?
  - Si non, la loi ne s'applique pas.
  - Si oui, se pose la question suivante:
- Les données à caractère personnel traitées sont-elles contenues dans un fichier ou appelées à y figurer?
  - Si non, la loi ne s'applique pas.
  - Si oui, la loi s'applique.

Notons enfin que la loi s'applique de manière pour ainsi dire modulée. Certaines dispositions, contenant les principes de base de la législation, s'appliquent toujours, sans distinction, dès que l'on rentre dans le champ d'application de la loi; tandis que d'autres dispositions ne s'appliquent pas dans certains cas. En effet, la loi prévoit certaines exceptions partielles, à savoir certaines situations qui ne sont pas soumises à certaines dispositions. Nous détaillerons ces exceptions ci-dessous.

§ 2. - Le champ d'application personnel

Sur ce point, la loi ne fait aucune distinction selon la nature ou la qualité du responsable du traitement: elle s'applique aussi bien aux personnes physiques que morales, tant publiques que privées, dès lors que celles-ci traitent des données à caractère personnel.

[33] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 65.
[34] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 65-68.

§ 3. – Les exceptions

La loi prévoit diverses exceptions, excluant de la sorte certains traitements de son champ d'application, tantôt de manière totale, tantôt partiellement – ce qui se réfère à l'application modulée de la loi évoquée ci-dessus. Nous ne nous attarderons que sur celles susceptibles d'intervenir en matière de santé publique, nous contentant d'envisager brièvement les autres exceptions, moins pertinentes s'agissant du sujet qui nous occupe.

A. Traitement effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques

Cette exception est totale – et c'est la seule –, l'ensemble des dispositions de la loi ne s'appliquant pas à ce type de traitement. Plusieurs conditions sont à respecter afin de pouvoir invoquer cette exception. Il faut tout d'abord que le traitement soit effectué par une personne physique, et non une personne morale ou une association. C'est ici que les considérations évoquées ci-dessus au sujet de la personne qui a la qualité de responsable du traitement dans des cas particuliers, prennent toute leur importance. En effet, si c'est la personne morale qui est qualifiée de responsable du traitement, elle ne peut invoquer cette exception. A l'inverse, une personne physique, membre d'une personne morale, mais qui au vu des circonstances est elle-même responsable du traitement, peut bénéficier de cette exception, moyennant le respect des autres conditions auxquelles elle est soumise.

C'est ainsi que la personne physique qui entend faire usage de cette exception, doit en outre prouver que le but du traitement se limite à l'exercice d'activités exclusivement personnelles et domestiques – par exemple, un agenda privé, ou un carnet d'adresses. Le fait que le traitement soit effectué au domicile de la personne physique n'a pas d'importance, c'est la finalité du traitement qui importe. Ainsi, un employé qui traite à son domicile des données pour des finalités de son entreprise, ne peut invoquer cette exception[35].

B. Traitement effectué aux seules fins de journalisme ou d'expression artistique ou littéraire

Cela est aisément concevable, la liberté de la presse doit être garantie et protégée, et ne peut être totalement anéantie au nom du respect de la vie privée. Un équilibre a donc dû être établi afin de concilier ces deux intérêts, cet équilibre consistant en une exception partielle soumise au principe de finalité. Ce n'est donc pas le statut du responsable du traitement qui importe, mais bien la finalité du traitement qu'il opère[36]. Ainsi, un journaliste ne peut en toutes circonstances traiter des données à caractère personnel en échappant à la loi, pour la seule raison tenant à sa qualité de journaliste. De la même manière, toute autre personne, sans être journaliste, peut être amenée à traiter

[35] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 72.
[36] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 76.

des données aux fins de journalisme et donc bénéficier du régime d'exception. De plus, pour pouvoir bénéficier de l'exception, le responsable doit agir aux *seules* fins de journalisme, d'expression artistique ou littéraire.

Cette exception n'est que partielle, et ne concerne que quatre aspects de la protection de la vie privée. Tout d'abord, en cas de données sensibles, judiciaires ou de santé – pour lesquelles les articles 6, 7 et 8 prévoient un régime plus strict, comme nous le verrons ci-dessous –, le traitement peut être réalisé s'il est nécessaire pour des finalités exclusivement journalistiques, littéraires ou artistiques, et s'il "se rapporte à des données rendues manifestement publiques par la personne concernée ou sur des données qui sont en relation étroite avec le caractère public de la personne concernée ou du fait dans lequel elle est impliquée" (art. 3, § 3, a)). Ensuite, l'obligation d'information prévue à l'article 9, ainsi que les droits d'accès et de correction des données des articles 10 et 12, peuvent être contournés s'ils sont susceptibles de compromettre la collecte des données, une publication en projet ou encore l'anonymat des sources d'informations. Enfin, certaines mentions ne doivent pas figurer dans la déclaration de traitement à remettre à la Commission de la protection de la vie privée.

C. Exceptions en matière de Sûreté de l'Etat, de services de renseignements et de police

Pour des motifs de sécurité, diverses exceptions sont accordées en faveur d'organismes de police, d'enquêtes, etc. N'étant que très peu pertinentes en matière de santé publique, nous ne les analyserons pas en détail ici.

D. Traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques

Sans être mentionné dans la liste des exceptions au champ d'application de la loi, un régime particulier est prévu pour le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques. En effet, plusieurs exceptions sont établies par la loi en faveur de pareil traitement. Ainsi, il peut être dérogé au principe de finalité (art. 4, § 1er, 2°: "*Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par le Roi (...)*"); à la règle selon laquelle les données ne peuvent être conservées plus longtemps que ce qui est nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées et traitées (art. 4, § 1er, 5°); à l'interdiction de principe de traiter des données sensibles, relatives à la santé ou judiciaires (art. 6, § 2, al. 1er, g), art. 7, § 2, k), et art. 8, § 2, e)); et à l'obligation d'information qui incombe au responsable du traitement lorsque les données ne peuvent être obtenues auprès de la personne concernée elle-même (art. 9, § 2, al. 2, a)).

Bien entendu, ces exceptions ne sont pas dépourvues de toute garantie, la loi prévoyant à chaque dérogation que celle-ci n'est possible que moyennant le respect des conditions fixées par le Roi, c'est-à-dire par arrêté royal. De plus, cet arrêté ne peut être adopté qu'après avis de la Commission de la protection de la vie privée. Diverses

garanties ont donc été instaurées par l'arrêté royal du 13 février 2001[37], dont nous analyserons le régime au cours des lignes qui suivent.

1) *La notion de traitement ultérieur à des fins historiques, statistiques et scientifiques*

Une première question qui se pose est de savoir à quels traitements exactement ce régime particulier s'applique. Que signifie l'expression "traitement ultérieur à des fins historiques, statistiques ou scientifiques"? La précision n'est pas sans importance, étant donné qu'un grand manque de clarté et bon nombre d'incertitudes règnent dans la pratique. La directive européenne n'offrant aucune définition qui puisse nous éclairer à ce sujet, c'est vers la recommandation du Conseil de l'Europe en matière d'enquête statistique[38] qu'il nous faut nous tourner.

Selon ce document, le traitement à des **fins statistiques** vise "toute opération de collecte et de traitement de données à caractère personnel nécessaire aux enquêtes statistiques ou à la production de résultat statistique". L'exposé des motifs précise que "la statistique a pour objet l'analyse des phénomènes de masse. Elle permet, grâce à un processus de condensation, de tirer une affirmation générale d'une série d'observations individuelles systématiques". Contrairement à ce que ces définitions pourraient donner à croire, "le terme de finalité statistique vise (…) non seulement la statistique publique mais également la statistique privée"[39].

La **recherche scientifique** est quant à elle définie au point 14 de l'exposé des motifs de la recommandation, comme visant à établir "des permanences, des lois de comportements ou des schémas de causalité qui transcendent tous les individus qu'ils concernent. Ainsi, elle vise à caractériser des phénomènes d'ensemble". Il en résulte que les enquêtes de population menées par les instituts scientifiques, tels que Louis Pasteur ou la Fondation Registre du Cancer, sont incluses dans la notion de fin scientifique[40]. En effet, le terme "scientifique" concerne non seulement le but, mais également la méthode de l'enquête[41].

Quant au terme **historique**, il renvoie "à des traitements de données à caractère personnel ayant pour finalité d'analyser un événement passé ou de permettre cette analyse"[42]. Si le critère de l'événement passé soulève de nombreuses interrogations dans la pratique, les auteurs s'accordent pour dire que "l'archivage par le responsable du

---

[37] Arrêté royal du 13 février 2001portant 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, chapitre II, *M. B.,* 13 mars 2001, www.moniteur.be.

[38] Recommandation n° R (97) 18F du 30 septembre 1997 du Comité des Ministres du Conseil de l'Europe aux Etats membres concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, http://www.coe.int.

[39] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 465.

[40] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 465.

[41] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 102.

[42] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 465.

traitement de ses propres fichiers n'est pas considéré comme une conservation à des fins historiques", tandis que le travail des généalogistes s'assimile à un tel traitement[43].

Il est important de signaler que, s'agissant de ces trois notions, si les données individuelles ne sont pas visées *a priori*, la connaissance des grands ensembles et des phénomènes de masse l'étant davantage, des dangers de détournement de finalité et de recoupement existent cependant, permettant l'identification des personnes concernées[44]. C'est pourquoi la prise en considération des traitements ultérieurs à des fins historiques, statistiques et scientifiques n'est en aucun cas dépourvue de pertinence en matière de traitement de données à caractère personnel.

Le régime particulier établi par l'arrêté royal ne vise que le **traitement ultérieur**, et non tout traitement à des fins de recherches historiques, statistiques ou scientifiques dans le cadre de la finalité initialement déclarée et légitime, lequel reste soumis au régime général de la loi. Sont donc uniquement visées les utilisations ou collectes secondaires, à l'exclusion des collectes initiales. En effet, la notion de traitement ultérieur "vise l'hypothèse où le responsable d'un traitement qui traite des données à caractère personnel dans le cadre de ses activités habituelles et légitimes souhaite les réutiliser lui-même ou les communiquer à un tiers, en vue d'une recherche scientifique, historique ou statistique"[45]. Il faut donc, pour que le régime de l'arrêté royal s'applique, qu'il s'agisse de données initialement collectées pour une finalité qui n'est pas de nature historique, statistique ni scientifique, et qui sont ultérieurement réutilisées pour des finalités de telle nature qui ne sont pas compatibles avec les finalités initiales[46]. Cela implique que l'on définisse également la notion de **compatibilité**, puisque si le traitement ultérieur est réalisé pour des finalités compatibles avec les finalités initiales, le régime de la loi restera applicable. Selon la doctrine, "une finalité compatible est une finalité que la personne concernée peut raisonnablement prévoir ou qu'une disposition légale prévoit"[47].

2) *Le régime particulier de l'arrêté royal*

Selon le régime général de la loi, les données à caractère personnel ne peuvent être traitées ultérieurement que de manière compatible avec les finalités du traitement initial (art. 4, § 1er, 2° de la loi). S'agissant du traitement ultérieur à des fins historiques, statistiques ou scientifiques, il sera réputé compatible avec les finalités initiales s'il respecte les conditions prévues par l'arrêté royal (art. 2, al. 1er AR). De la même manière, "la conservation des données à caractère personnel à des fins historiques, statistiques ou scientifiques, visée à l'article 4, § 1er, 5°, deuxième phrase, de la loi, est autorisée aux conditions déterminées" par l'arrêté royal (art. 2, al. AR). Ces conditions consistent en une réglementation en cascade, selon laquelle prévaut le traitement de

---

[43] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 465.

[44] C. DE TERWANGNE et S. LOUVEAUX, "Protection des données à caractère personnel: l'application de la directive européenne", *in Actualités du droit des technologies de l'information et de la communication,* formation permanente de la commission Université-Palais, Liège, fév. 2001, vol. 45, pp. 7 et s.

[45] Rapport au Roi, *M.B.*, 13 mars 2001, p. 17.

[46] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 103.

[47] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, pp. 465-466.

données anonymes, puis de données codées, et enfin de données non codées; cette réglementation se faisant de plus en plus stricte dans la mesure où les traitements sont de plus en plus attentatoires à la vie privée.

En effet, l'article 3 de l'arrêté royal énonce le principe général selon lequel "le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques est effectué à l'aide de données anonymes". C'est seulement lorsque pareil traitement ne permet pas d'atteindre les finalités historiques, statistiques ou scientifiques que le traitement de données codées sera autorisé, moyennant le respect des conditions fixées par l'arrêté royal (art. 4 AR). Il en va de même pour l'utilisation de données non codées: celle-ci n'est permise que lorsque les finalités ne peuvent être atteintes par un traitement de données codées, l'arrêté royal entourant cette autorisation de garanties supplémentaires (art. 5 AR).

Lorsque c'est possible, il faut donc travailler avec des **données anonymes**, à savoir des données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable, et qui ne consistent donc pas en données à caractère personnel (cf *supra*, définition de la notion de données à caractère personnel). Il doit donc être définitivement impossible de relier ces données à une personne[48]. L'anonymat doit être véritable: "les données d'identification doivent être effacées"[49].

Il existe cependant des cas dans lesquels il est nécessaire de travailler avec des données reliées à des personnes identifiables. C'est le cas, par exemple, de ce que l'on appelle "*longitudinal research*"[50], ou de recherches nécessitant le suivi d'un même individu afin de comparer certains faits ou résultats, ou encore de recherches requérant l'établissement de liens entre des données concernant une même personne[51]. L'arrêté royal autorise alors l'utilisation de **données codées**, à savoir "les données à caractère personnel qui ne peuvent être mises en relation avec une personne identifiée ou identifiable que par l'intermédiaire d'un code" (art. 1er, 1° AR). Trois obligations incombent alors au responsable du traitement ultérieur. Tout d'abord, il doit indiquer dans la déclaration qu'il remet à la Commission de la protection de la vie privée (cf. *infra*), les motifs pour lesquels il ne peut réaliser ce traitement à l'aide de données anonymisées (art. 4, al. 2 AR). Ensuite, il ne peut entreprendre aucune action visant à convertir les données codées en données non codées (art. 6 AR). Enfin, afin de pouvoir se faire communiquer les données par le responsable du traitement initial, il doit présenter l'accusé de réception d'une déclaration complète, délivré par la Commission (art. 13 AR). S'agissant du codage des données, il doit être de telle nature que les données à caractère personnel, avant d'être traitées à des fins historiques, statistiques ou scientifiques, soient déliées de tout élément qui permettrait l'identification de la personne concernée. En outre, la clé du codage ne peut en aucun cas être communiquée[52].

L'arrêté royal envisage trois hypothèses, dont la première consiste en l'utilisation ultérieure par le responsable du traitement initial (art. 8). Dans ce cas, soit il code lui-même les données, soit il confie le traitement ultérieur à un sous-traitant qui code lui-

[48] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 106.
[49] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 466.
[50] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 104.
[51] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 466.
[52] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 108.

même les données, soit enfin il confie le codage des données à une organisation intermédiaire afin de pouvoir lui-même réutiliser ces données par la suite à des fins historiques, statistiques ou scientifiques. Cette organisation intermédiaire agit alors en tant que sous-traitant, l'arrêté royal prévoyant en son article 11 qu'elle doit être indépendante du responsable du traitement ultérieur, et ce afin de pouvoir refuser de donner la clé du code au destinataire des données[53]. Précisons que la loi elle-même prévoit des garanties quant au choix du sous-traitant et de la relation qu'il entretient avec le responsable du traitement (cf. *infra* art. 16 de la loi).

Un second cas de figure est celui du traitement ultérieur par des tiers, pour lequel l'article 9 de l'arrêté royal impose que le codage des données soit effectué par le responsable du traitement initial ou par une organisation intermédiaire, préalablement à leur transmission. Il s'agit par exemple du cas de sociétés qui vendent leurs fichiers à une société de marketing à des fins de profilage[54]. Enfin, l'article 10 prévoit le cas du traitement ultérieur à la suite de la transmission par plusieurs responsables du traitement au(x) même(s) tiers. Par exemple, un traitement à des fins statistiques est effectué par l'U.P.E.A. (Union professionnelle des entreprises d'assurances) sur base de données provenant de diverses compagnies d'assurances. C'est également le cas de sociétés qui demandent aux médecins généralistes de leur envoyer les données de leurs patients. Dans ce cas, les données doivent être codées avant leur transmission par une organisation intermédiaire, indépendante. Celle-ci sera alors, pour l'opération du codage des données, responsable d'un nouveau traitement, et soumise au régime général de la loi. Une difficulté réside dans le fait que, en l'absence d'une précision au sein de l'arrêté royal selon laquelle les données seraient rassemblées avant d'être communiquées au tiers, les différents transmetteurs ne sont pas toujours en mesure de savoir qu'ils sont plusieurs à transmettre ces données, et qu'ils sont donc tenus de ne pas les communiquer directement au tiers, mais de les transmettre préalablement à une organisation intermédiaire[55].

Dans ces trois hypothèses, une garantie générale est établie par l'article 12, lequel impose au responsable du traitement initial et à l'organisation intermédiaire qui codent les données, de prendre "des mesures techniques et organisationnelles adéquates, afin d'empêcher la conversion des données codées en données non codées". S'ajoutent à cette disposition des garanties spécifiques lorsque pareil traitement est réalisé sur base de données sensibles, médicales et judiciaires. L'article 14 de l'arrêté royal impose en effet au responsable du traitement initial de communiquer à la personne concernée certaines informations relatives au traitement ultérieur. Si l'article 15 envisage la possibilité d'une exemption de cette obligation, lorsque son respect est impossible ou implique des efforts disproportionnés, l'article 16 assortit toutefois cette exemption d'une autre obligation, consistant en la mention d'informations supplémentaires dans la déclaration à remettre à la Commission. Celle-ci sera alors en mesure, dans un certain délai, d'émettre toute recommandation qu'elle jugera utile, et de soumettre le traitement ultérieur à certaines conditions supplémentaires. Pareille recommandation n'a certes aucune valeur

[53] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, pp. 466-467.
[54] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 467.
[55] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 467.

obligatoire, mais "en cas de litige, elle peut créer une présomption de légalité ou d'illégalité"[56]. Notons également qu'une exemption est prévue en faveur de l'organisation intermédiaire qui est à la fois une autorité administrative chargée explicitement par ou en vertu de la loi de rassembler et de coder les données et soumise, à cet égard, à des mesures spécifiques visant à protéger la vie privée, instituées par ou en vertu de la loi (art. 15, al. 2 AR). Sont ici visées les institutions telles que la Banque-carrefour de la sécurité sociale.

Il est enfin des cas dans lesquels la réalisation des finalités historiques, statistiques et scientifiques ne sera possible qu'en traitant des **données à caractère personnel non codées**. Si pareil traitement comporte de nombreux avantages pour le responsable du traitement, qui pourra travailler plus vite sur base de données déjà collectées et dont la fiabilité a déjà été vérifiée par le responsable du traitement initial, il est également porteur de risques, la personne concernée perdant une certaine maîtrise du traitement de ses données personnelles. C'est au nom de ces risques plus importants que l'arrêté royal prévoit des règles et conditions plus strictes que dans le cas de données codées. Ce régime repose sur le consentement informé de la personne concernée, étant assorti d'obligations complémentaires incombant au responsable du traitement ultérieur.

En premier lieur, celui-ci devra justifier dans sa déclaration auprès de la Commission de la protection de la vie privée, des motifs pour lesquels le traitement ultérieur de données codées ne lui permet pas d'atteindre les finalités historiques, statistiques et scientifiques (art. 5, al. 2 AR). L'arrêté royal lui impose en outre de communiquer un certain nombre d'informations à la personne concernée (art. 18). S'ajoute à cela l'exigence du consentement de la personne concernée, lequel doit être préalable au traitement ultérieur, et exprès. Ainsi, contrairement à la notion de consentement de la personne concernée telle que présente dans la loi, un consentement implicite ne sera pas suffisant dans le cas du traitement ultérieur de données non codées. Si l'arrêté royal ne précise pas que le consentement doit être écrit, il est toutefois préférable d'opter pour cette voie, afin de s'assurer la preuve du consentement exprès de la personne concernée – la charge de cette preuve incombant au responsable du traitement ultérieur[57].

En son article 20, l'arrêté royal prévoit toutefois deux cas dans lesquels une exemption aux obligations d'information et d'obtention du consentement se justifie. Il s'agit d'une part de la situation dans laquelle les données en question sont manifestement rendues publiques par la personne concernée ou sont en "relation étroite avec le caractère public de la personne concernée ou des faits dans lesquels celle-ci est ou a été impliquée" – comme par exemple la recherche au moyen d'archives, les données issues de condamnations pénales prononcées dans le passé contre un homme politique, les données portant sur des personnes ordinaires impliquées dans un événement public et relatives à cet événement, ou encore les noms des signataires d'une pétition. La seconde exemption vaut lorsque l'obligation de consentement informé se révèle impossible, ou implique des efforts disproportionnés, ce qui vise notamment "les traitements de grandes quantités de données à caractère personnel non codées dans un environnement non automatisé", ces

[56] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 468.
[57] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 468.

circonstances rendant une opération de codage des données inimaginable[58]. Le responsable de pareil traitement sera alors tenu de compléter sa déclaration auprès de la Commission de la vie privée avec les informations énumérées à l'article 21, ce qui mettra cette dernière en mesure d'émettre une éventuelle recommandation pouvant être assortie de conditions supplémentaires à l'exécution du traitement.

Une dernière garantie entourant tout traitement ultérieur à des fins historiques, statistiques ou scientifiques concerne la **publication des résultats**. L'article 23 de l'arrêté royal interdit en effet la publication des résultats de pareil traitement sous une forme qui permette l'identification de la personne concernée, assortissant cette interdiction de principe de deux exceptions. D'une part, si la personne concernée a consenti à une telle publication, et qu'il n'est pas porté atteinte à la vie privée de tiers, et d'autre part lorsque les données publiées sont manifestement rendues publiques par la personne concernée ou étroitement reliées au caractère public de celle-ci ou des faits dans lesquels elle est impliquée.

Notons enfin qu'une exception est prévue à l'article 24 de l'arrêté royal, dispensant les services de sûreté de l'Etat, le service général du renseignement et de la sécurité des forces armées, l'autorité de sécurité, les officiers de sécurité et le comité permanent de contrôle des services de renseignement set son service d'enquête, du régime du chapitre II de l'arrêté royal, lorsque le traitement ultérieur à des fins historiques, statistiques ou scientifiques est nécessaire à l'exercice de leur mission.

Section III. – Le champ d'application territorial

En vertu des règles de droit international public et privé, une loi belge ne peut s'appliquer à toutes les situations existant dans d'autres pays. Pourtant, les nouvelles technologies et la mondialisation permettent et encouragent le traitement dans un certain pays de données provenant d'un autre pays, ainsi que la communication transfrontalière de données à caractère personnel. C'est pourquoi la loi belge prévoit certaines règles visant à protéger les données à caractère personnel au-delà de son territoire, tout en n'excédant pas ses pouvoirs. C'est l'objet de l'article 3*bis* de la loi du 8 décembre 1992.

Une directive européenne ayant été adoptée en la matière et donc transposée dans tous les Etats membres de l'Union européenne, ceux-ci sont sensés assurer un niveau égal de protection. C'est pourquoi la loi réglemente principalement les situations transfrontalières impliquant des Etats non-membres de l'UE.

Deux critères de rattachement – c'est-à-dire des critères déterminant l'application de la loi belge à un traitement comportant des caractéristiques transfrontalières avec des pays non-membres de l'UE – sont ainsi établis, le premier étant celui du lieu d'établissement fixe du responsable du traitement. Pour y satisfaire, il faut non seulement que le traitement soit effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement, mais aussi que cet établissement soit situé sur le territoire belge. S'agissant du premier élément de ce premier critère, un traitement peut être effectué par un groupe de sociétés établies dans différents pays, ce traitement étant centralisé sur un même territoire, et risque donc de se voir appliquer

[58] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 468.

l'ensemble des lois nationales des territoires sur lesquels ces sociétés sont situées. Dans pareil cas, "seule la loi du pays où est située la société qui traite les données est applicable"[59], même si les autres sociétés du groupe profitent de ce traitement. Ce n'est que si ces autres sociétés effectuent un nouveau traitement à l'aide des données centralisées qu'elles seront soumises à leurs lois nationales. Le critère du lieu d'établissement fixe du responsable du traitement contient donc une autre condition essentielle, à savoir que "l'établissement doit participer au traitement des données dans le cadre de ses activités et n'est soumis à la loi que dans la mesure du traitement qu'il opère sur les données"[60]. Précisons en outre que, selon l'exposé des motifs, "l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable"[61].

Si ce premier critère ne peut s'appliquer, l'article 3*bis*, 2° prévoit un second critère de rattachement, à savoir celui des moyens utilisés. Ce critère s'applique lorsque le responsable du traitement n'est pas établi de manière permanente sur le territoire de l'UE, et utilise des moyens situés sur le territoire belge. Le terme "moyens" recouvre, selon l'exposé des motifs, "tout équipement possible, tels que les ordinateurs, les appareils de télécommunication, les unités d'impression, etc., à l'exclusion, formulée explicitement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routes, etc."[62]. Si cette définition, issue de la directive européenne, parait fort large, il convient de ne pas y conférer une interprétation extensive, laquelle aboutirait à la conséquence absurde et irréaliste selon laquelle tout traitement situé en dehors de l'UE serait soumis à la loi belge dès lors qu'il présenterait un lien matériel, si minime soit-il, avec le territoire de la Belgique. Il convient au contraire de retenir l'application de l'article 3*bis*, 2° dans seulement deux cas, à savoir: lorsque le responsable cherche délibérément à contourner les lois nationales et délocalise pour ce faire son établissement dans un pays tiers tout en utilisant encore certains moyens sur le territoire belge; et lorsque le responsable réalise, par des moyens propres situés sur le territoire belge, un flux de données vers le pays tiers où il traite les données. Le but de cette disposition est donc d'éviter que la législation ne soit contournée, ce qui priverait la personne concernée de toute protection[63]. Notons que dans ce cas, la loi prévoit que le responsable du traitement doit désigner un représentant en Belgique.

---

[59] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 382.

[60] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, pp. 382-383.

[61] Exposé des motifs, *Doc. parl.,* Ch. repr., sess. ord. 1997-1998, n° 1566/1, considérant 19.

[62] Exposé des motifs, *Doc. parl.,* Ch. repr., sess. ord. 1997-1998, n° 1566/1, p. 27.

[63] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 383.

Section IV. – Le champ d'application temporel

Cet aspect du champ d'application de la loi ne semble présenter qu'un faible intérêt, en ce sens que la loi étant entrée en vigueur depuis maintenant plusieurs années, elle s'applique à la grand majorité des traitements actuellement en cours.

Chapitre II. – Comment vérifier le respect de la protection de la vie privée?

Résumons-nous. Si nous sommes en présence d'un véritable traitement de données à caractère personnel au sens de la loi, dont le responsable fait partie des personnes visées par la loi, et qui ne correspond à aucun des cas d'exception prévus par celle-ci, la loi nous est applicable. Que cela signifie-t-il? A quelles conditions la loi soumet-elle la réalisation d'un traitement de pareilles données? Quelles sont les différentes obligations qui en découlent? Enfin, quels sont les mécanismes de contrôle destinés à vérifier que la loi est correctement appliquée et respectée?

Section I^{ère}. – Les conditions de licéité du traitement de données à caractère personnel

Le chapitre II de la loi sur la protection de la vie privée traite des conditions de licéité des traitements de données à caractère personnel. Certaines conditions sont générales et s'appliquent à tout traitement inclus dans le champ d'application de la loi (art. 4 et 5), tandis que d'autres sont spécifiques aux traitements de certains types de données, à savoir les données dites sensibles (art. 6), les données relatives à la santé (art. 7) et les données judiciaires (art.8). En effet, un régime plus strict est prévu pour le traitement de ces données particulières, au nom du lien étroit qu'elles entretiennent avec la vie privée et des risques de discrimination qui en découlent. Notons que ce degré supérieur de protection est sans préjudice de l'application des principes généraux en matière de licéité des traitements de données à caractère personnel. Les traitements de données particulières y restent soumis, et ce de manière cumulative.

§ 1er. – Les conditions générales

Les conditions générales, à savoir celles qui s'appliquent à tout type de traitement, tiennent d'une part à la qualité du traitement des données, et d'autre part à l'admissibilité ou l'acceptabilité du traitement.

A. Les conditions relatives à la qualité du traitement des données (art. 4)

L'article 4 énonce cinq principes auxquels doivent se conformer les traitements de données à caractère personnel pour être licites. Le second paragraphe de cet article précise que c'est au responsable du traitement qu'il incombe d'assurer le respect de ces conditions.

Tout d'abord, les données doivent être traitées **loyalement et licitement**, le premier adverbe se référant à l'exigence de transparence – concrétisée par l'obligation d'information de la personne concernée, et présente dans d'autres dispositions de la loi, telles que celle relative à la conservation des données (cf. *infra*) – le second rappelant simplement que toutes les autres dispositions de la loi doivent être respectées afin d'être en présence d'un traitement licite.

Doit en outre être respecté le **principe de finalité**, véritable pierre angulaire de la réglementation de la protection de la vie privée en matière de traitement de données à caractère personnel. Ainsi, les données doivent être "collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables". Nous avons déjà évoqué cette règle lors de l'examen du traitement ultérieur à des fins historiques, statistiques et scientifiques, mais nous l'expliquerons plus en détail au cours de ce paragraphe. Le principe de finalité peut être subdivisé en trois sous-principes, dont le premier est celui de la description des finalités, lequel exige que le traitement soit effectué pour une ou plusieurs finalités précisément déterminées (la loi emprunte les termes de finalités déterminées et explicites), et ce préalablement à la collecte des données. Sont ainsi considérés comme illicites les traitements effectués pour toutes finalités utiles, sans objet suffisamment déterminé. En outre, la jurisprudence exige que les finalités soient décrites de telle sorte qu'elles soient compréhensibles pour chacun, en particulier pour le citoyen moyen[64].

Le second sous-principe est celui de la légitimité des finalités, ce qui implique qu'elles ne peuvent violer les droits et libertés fondamentaux sans raison légale. Une fois de plus, c'est une position d'équilibre qu'il convient de maintenir entre les différents intérêts en jeu. Il est en général accepté que pour être légitime, une finalité doit être en lien avec l'activité sociale du responsable du traitement[65].

Quant au dernier sous-principe, à savoir celui de l'usage compatible (les données ne pouvant être traitées ultérieurement de manière incompatible avec les finalités du traitement initial), il convient de ne pas lui conférer une portée trop stricte. En effet, toutes les finalités possibles d'un traitement ne peuvent être anticipées dès le début, et il serait fastidieux d'exiger du responsable du traitement de recommencer toutes les démarches à accomplir pour un nouveau traitement. Ainsi, si ce principe implique que tout traitement ultérieur soit confronté aux finalités du traitement initial, la doctrine considère qu'il n'empêche pas que les traitements évoluent en comparaison avec les finalités dont il a été donné connaissance lors du traitement initial. Ce principe exige plutôt que lorsque l'on change de finalité, le traitement ultérieur soit soumis de manière complète à toutes les règles de protection. Autrement dit, un traitement ultérieur qui en

[64] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 117-118.
[65] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 118.

soi n'est pas compatible avec la finalité initiale, sera dans la pratique autorisé dans la plupart des cas, pour autant qu'il soit légitime, ce qui implique qu'il respecte toutes les dispositions de la loi[66]. Notons que la loi précise que pour juger de la compatibilité du traitement ultérieur, il convient de tenir compte de tous les facteurs pertinents. Si deux de ces facteurs sont cités dans la disposition légale – à savoir les prévisions raisonnables de la personne intéressée, dont l'appréciation relève d'une question de fait[67]; et les dispositions légales ou réglementaires applicables[68] – d'autres facteurs sont susceptibles d'influencer la compatibilité du traitement ultérieur, comme la nature des données, l'intérêt du responsable du traitement, ou encore les risques potentiels d'atteinte à la vie privée[69]. Ce principe de l'usage ultérieur compatible donne toute son importance à la notion d'information de la personne concernée. Si, lors du traitement initial, celle-ci a été informée de manière complète et précise sur les possibilités de traitements futurs de ses données à caractère personnel, et des finalités connexes du traitement initial, un traitement ultérieur pourra plus facilement être considéré comme compatible avec les finalités initiales du traitement.

La troisième condition relative à la qualité du traitement des données à caractère personnel exige que ces dernières soient "adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement" (art. 4, § 1er, 3°). Il s'agit d'exiger l'existence d'un lien nécessaire et suffisant entre l'information recueillie et la finalité du traitement. Le terme "adéquates" implique que le traitement contienne suffisamment de données pour réaliser les objectifs établis, la pertinence des données devant s'apprécier au cas par cas, et non *in abstracto*. L'exigence de la non excessivité des données empêche les comportements consistant à collecter un maximum de données, "au cas où". Le caractère excessif ou non des données s'apprécie par rapport aux finalités du traitement. Toutes ces exigences peuvent être rassemblées en un **principe de proportionnalité**, lequel exige qu'une considération des différents intérêts en présence soit opérée lors du choix des données.

La loi exige en outre que les données soient **exactes**, et si nécessaire mises à jour, ce qui consiste en une obligation de souci de qualité permanent. Toutes les mesures raisonnables doivent être prises par le responsable du traitement afin de se conformer à ce devoir, le critère de référence étant celui du responsable normalement prudent et diligent.

---

[66] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 120-121.

[67] Ainsi par exemple, les données de l'administration universitaire et traitées à cette fin ne peuvent être transférées à des tiers à des fins de direct marketing, cette finalité n'étant pas compatible avec l'administration universitaire. De la même manière, des données traitées pour l'administration des salaires ne peuvent être utilisées pour prendre des sanctions disciplinaires sur base des prestations des travailleurs. Par contre, les données relatives aux diplômes ou aux capacités professionnelles d'un membre du personnel pourront être utilisées pour d'autres décisions politiques comme la sélection, le planning personnel ou la promotion. (Voy. D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 122.)

[68] Un exemple de l'application de ce facteur est l'usage par l'autorité de données concernant les inscriptions des véhicules pour un système relatif au permis de conduire avec des points de sanction. (Voy. D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 122.) Cette disposition est toutefois critiquable, voy. Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 385.

[69] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 121-122.

Enfin, une dernière condition tient à la **conservation des données** sous une forme permettant l'identification des personnes concernées, qui ne peut excéder le temps nécessaire à la réalisation des finalités du traitement initial.

B. Les conditions de légitimité du traitement de données à caractère personnel

Il ne suffit pas de respecter les conditions relatives à la qualité du traitement des données à caractère personnel pour que le traitement soit licite et légitime. Encore faut-il pouvoir fonder le traitement sur une des situations décrites à l'article 5 de la loi. En effet, celui-ci énonce, de manière limitative, les cas dans lesquels pareil traitement est permis ou admissible, autrement dit les cas dans lesquels il peut être effectué. Le législateur a de la sorte estimé que, dans ces cas-là, le principe de proportionnalité est *a priori* respecté, un équilibre existant entre les intérêts de la personne concernée et ceux du responsable du traitement. Notons que, juridiquement, le caractère limitatif d'une énumération a pour conséquence que les situations énoncées doivent être interprétées restrictivement.

Précisons également que les conditions de l'article 4, 2° et celles de l'article 5 s'appliquent cumulativement. Le respect d'un article n'emporte pas automatique celui de l'autre. Ainsi par exemple, le consentement de la personne concernée ne permet pas nécessairement de légitimer la finalité du traitement, même si ce sera souvent le cas[70].

1) Consentement de la personne concernée

La première situation dans laquelle le traitement est autorisé vise le consentement indubitable de la personne concernée (art. 5, a)). Plusieurs conditions sont à réunir pour pouvoir invoquer cette possibilité. Il faut tout d'abord que le consentement soit **indubitable**, c'est-à-dire qu'on ne puisse lui attribuer qu'une seule signification. Le fait qu'il ne puisse y avoir qu'une seule interprétation possible n'emporte cependant pas l'exigence de l'écrit, pareil consentement pouvant être donné oralement. Le responsable du traitement prudent se procurera toutefois un consentement écrit, afin d'éviter toute contestation ultérieure[71]. Ce consentement doit en outre être **informé**, ce qui implique que la personne concernée consente en connaissance de cause, étant en possession de toutes les informations nécessaires à sa décision. Le contenu de cette information dépend des circonstances du cas d'espèce, même si l'article 9, traitant du droit à l'information de la personne concernée, offre certaines indications à ce sujet. Il va de soi que ce consentement peut être **retiré à tout moment**, sans toutefois que le retrait puisse agir de manière rétroactive. Enfin, il ne peut être consenti en termes généraux, l'accord devant porter sur des traitements clairement et **précisément déterminés**[72].

---

[70] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 384.
[71] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 129.
[72] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 130.

2) Exécution d'un contrat ou de mesures précontractuelles

Le traitement de données à caractère personnel est en outre permis lorsqu'il est "nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci" (art. 5, b)). Le traitement doit donc être nécessaire à l'exécution ou à la conclusion d'un accord, ce qui implique que la finalité du traitement doit viser l'essence même des mesures précontractuelles ou de l'objet des prestations contractuelles. Il faut en outre que la personne concernée soit partie à l'accord, ce qui exclut par exemple l'invocation de cette disposition par une banque en vue de traiter les données à caractère personnel de bénéficiaires de chèques postaux dans le cadre du trafic financier[73]. Précisons enfin que les traitements nécessaires à l'exécution de mesures précontractuelles ne sont permis que lorsque ces mesures sont prises à la demande de la personne concernée.

3) Respect d'une obligation légale

Si le responsable du traitement est tenu, en vertu de la loi, d'un décret ou d'une ordonnance, d'effectuer le traitement de données à caractère personnel, ce traitement sera licite, moyennant bien sûr le respect des autres conditions énumérées ci-dessus et relatives à la qualité du traitement des données. Cette disposition s'applique par exemple aux employeurs tenus de tenir des registres de leurs membres du personnel à la disposition des inspecteurs sociaux. De même, les employeurs sont également tenus de communiquer certaines données concernant leur personnel aux institutions de la sécurité sociale.

4) Sauvegarde de l'intérêt vital de la personne concernée

Cette disposition vise les traitements qui sont essentiels à la vie de la personne concernée. Afin de ne pas laisser la porte ouverte aux abus, il convient d'interpréter cette disposition de manière particulièrement restrictive, la limitant aux questions de vie ou de mort, en présence d'une nécessité médicale urgente. Cela dit, même si dans la plupart des cas visés la personne concernée ne sera pas en mesure de consentir, le responsable du traitement n'est pas tenu de prouver l'impossibilité physique ou juridique dans laquelle se trouve la personne concernée. En effet, certaines situations présentent une nécessité de traiter les données tellement urgente que le consentement ne sera pas demandé. Il s'agit par exemple des cas de catastrophes de grande échelle nécessitant des mesures d'assistance ou de secours, tels que les incendies[74].

5) Mission d'intérêt public

Le traitement de données à caractère personnel sera en outre autorisé lorsqu'il est "nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les

[73] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 131.
[74] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 132-133.

données sont communiquées" (art. 5, e)). Ces tâches d'intérêt public sont souvent la conséquence de dispositions légales, comme par exemple la loi concernant les services de sécurité et de renseignements. Sont ainsi visés les traitements poursuivis dans le secteur public au sens large, dans lequel on retrouve les principes administratifs de légalité, spécialité et proportionnalité[75], principes que comprennent les règles de légitimité des traitements de données à caractère personnel.

6) Intérêt légitime du responsable du traitement

Cette disposition joue en quelque sorte le rôle de catégorie résiduaire. En effet, s'il est estimé dans les autres cas qu'il existe *a priori* un équilibre entre les intérêts en présence, le principe de proportionnalité devra ici se vérifier *in concreto.* Le traitement doit être nécessaire "à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées", et ne sera permis que si l'intérêt ou les droits et libertés fondamentaux de la personne concernée ne prévalent pas (art. 5, f)). Notons que l'équilibre qu'il convient de maintenir entre les intérêts en présence – à savoir ceux du responsable du traitement ou de tiers, et ceux de la personne concernée – peut être rétabli, en cas de déséquilibre, par l'adoption de mesures complémentaires, telles que la possibilité de s'opposer au traitement[76].

§ 2. – Le traitement de catégories particulières de données à caractère personnel

Certaines données touchent plus intimement à la vie privée, entraînant de la sorte un plus grand nombre de risques de violation de celle-ci, ce qui justifie un régime plus strict s'imposant au traitement de ces données particulières. La loi regroupe ces données en trois catégories, à savoir les données dites sensibles, les données relatives à la santé, et les données judiciaires.

Si le traitement de ces données particulières est en principe interdit, de nombreuses exceptions permettent toutefois de les traiter, moyennant le respect des conditions fixées par le Roi (art. 6, § 4, 7, § 3 et 8, § 4 de la loi). C'est pourquoi l'arrêté royal d'exécution soumet, en son article 25, les traitements visés aux articles 6 à 8 de la loi au respect de certaines règles, obligeant le responsable du traitement à prendre certaines mesures supplémentaires. Ces mesures étant communes aux trois catégories de données particulières, nous les examinerons ci-dessous avant d'entamer l'analyse de chacune de ces catégories.

Tout d'abord, le responsable du traitement est tenu de désigner les catégories de personnes ayant accès aux données à caractère personnel, cette désignation devant comporter une description précise de leur fonction par rapport au traitement des données visées (art. 25, 1° AR). Le cas échéant, ce sera le sous-traitant qui effectuera pareille désignation. Il est donc exigé que les personnes soient désignées par leur fonction, leur

[75] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 384.
[76] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 134.

compétence par rapport au traitement. Ce n'est donc pas une liste nominative qui doit être établie. D. De Bot suggère à ce propos, tout comme l'a fait la Commission de la protection de la vie privée[77], que deux listes soient érigées: l'une mentionnant les profils et fonctions ayant accès aux données, l'autre désignant des personnes déterminées[78]. Cette disposition permet de pourvoir le traitement de données particulières d'un système de contrôle de l'accès aux données à caractère personnel, ce qui garantit un certain niveau de protection et de surveillance.

Le responsable du traitement, ou son sous-traitant, doit tenir cette liste des personnes habilitées à accéder aux données à la disposition de la Commission de la protection de la vie privée. L'ancienne version de la loi prévoyait que la liste devait également être accessible à la personne concernée, mais cette obligation a été abandonnée pour plusieurs raisons. Non seulement cela demandait des efforts disproportionnés et déraisonnables, mais en plus le risque était grand de voir les personnes ayant accès aux données soumises à diverses pressions, certaines données – comme par exemple les données judiciaires – étant convoitées par de nombreux tiers[79].

L'article 25, 3° de l'arrêté royal impose en outre au responsable du traitement de veiller à ce que ces personnes soient tenues à une obligation de confidentialité, que ce soit légalement, statutairement ou contractuellement. Cela signifie qu'une disposition déontologique ne suffit pas, n'ayant pas force obligatoire. Ainsi, en l'absence de secret professionnel légal applicable, il conviendra d'imposer le devoir de confidentialité dans les statuts ou dans les contrats de travail. Une critique peut toutefois être adressée à cette disposition, celle-ci ne prenant pas en compte le fait que certaines données n'aient pas de caractère confidentiel, comme c'est le cas de la collecte d'informations révélant l'appartenance politique d'élus, ces personnes ayant fait campagne et donc manifestement rendu publiques ces données. Les personnes qui utilisent ces informations doivent-elles être tenues à un devoir de confidentialité? Selon certains auteurs, "imposer le secret concernant des données de notoriété publique heurte la logique", l'article 25, 3° de l'arrêté royal ne conférant pas lui-même aux données particulières un caractère confidentiel, mais prescrivant d'imposer le secret aux personnes accédant à ces données lorsque le caractère confidentiel existe, ou lorsque la personne concernée n'entend pas rendre ces données publiques[80].

Enfin, une mention particulière s'ajoute à l'obligation d'information qui incombe au responsable du traitement en vertu de l'article 9 de la loi, à savoir celle de la base légale ou réglementaire autorisant le traitement de données particulières. Cette mention doit également figurer dans la déclaration auprès de la Commission de la protection de la vie privée, visée à l'article 17, § 1er de la loi. La base légale peut être trouvée dans les articles 6 à 8 de la loi, ou dans toute autre loi particulière, tandis que la base réglementaire vise les dispositions des arrêtés royaux.

---

[77] Avis 8/99 du 8 mars 1999 de la Commission de la protection de la vie privée, http://www.privacycommission.be.
[78] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 178.
[79] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 179.
[80] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 459.

§ 3. – Le traitement des données dites sensibles

L'expression "données sensibles" vise les données à caractère personnel "qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle" (art. 6, § 1er, al. 1er). Ces données étant estimées susceptibles d'être à l'origine de diverses discriminations[81], la loi ne permet leur traitement que moyennant le respect de certaines conditions, ou plutôt elle en interdit le traitement mais assortit la règle d'exceptions. Avant d'examiner le régime juridique auquel sont soumises ces données sensibles, il convient de définir cette notion et de déterminer précisément ce que l'on entend par elle.

A. Que recouvre la notion de "données sensibles"?

D. De Bot divise l'énumération légale en deux catégories, dont la première concerne les données qui révèlent l'information sensible, à savoir l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques et l'appartenance syndicale. Le lien exigé est moins strict que dans l'ancienne version de la loi, qui empruntait les termes de données "relatives" aux informations sensibles. En effet, il suffit aujourd'hui que l'information sensible puisse être déduite des données, sans que celles-ci se rapportent nécessairement à pareille information, pour pouvoir considérer ces données comme sensibles au sens de la loi[82]. Cela n'exclut cependant en aucune manière les données qui concernent directement l'information sensible. Simplement, la notion de données sensibles est de la sorte élargie. Certains auteurs dénoncent toutefois cette interprétation qu'ils qualifient d'absurde. En effet par exemple, "si un fichier relatif à des mauvais payeurs comporte des données relatives à M. Ben Ali ou Mme Mokambe, ces informations deviennent *a priori* interdites de traitement puisqu'elles "révèlent" assurément, par le nom des personnes concernées, une origine raciale ou ethnique. Il en est de même des traitements permettant l'exécution d'un virement au bénéfice d'un syndicat portant la mention "cotisation 1999" qui révèle sans doute possible l'appartenance syndicale"[83]. Le législateur a cependant voulu éviter ces excès, exigeant que la notion de données révélant l'information sensible soit interprétée de manière raisonnable: pour pouvoir être considérée comme donnée sensible au sens de la loi, le caractère sensible doit pouvoir être déduit avec certitude, ou selon une probabilité quasi certaine[84]. Ainsi, la commande d'un exemplaire de la Bible ou du Coran ne révèle pas avec certitude les convictions religieuses, et ne constitue donc pas une donnée sensible. Par contre, les opinions politiques peuvent être déduites avec une vraisemblable certitude

[81] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Commentaire des articles, *Doc. Parl.,* Ch. repr., sess. ord.1990-1991, n° 47K1610001 du 6 mai 1991, p. 11, http://www.lachambre.be.
[82] Exposé des motifs, pp. 33-34.
[83] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 386.
[84] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 138.

de l'inscription d'une personne à la liste d'un parti politique. Des critiques continuent toutefois d'être adressées à l'explication de cette notion de "révélation", exempte de toute distinction d'intensité, ainsi que de précision quant à l'appréciation objective ou subjective de ce concept[85].

La seconde catégorie de données sensibles exige cette fois un lien plus strict entre les données et l'information sensible, la loi empruntant les termes de données "relatives à la vie sexuelle". Pareilles données doivent donc concerner directement la vie sexuelle, et non seulement être en mesure de révéler celle-ci. C'est ainsi qu'un abonnement à certains périodiques ne peut être une donnée sensible, tandis que le fait d'être membre d'une association militant pour les homosexuels et lesbiennes devra être qualifié de donnée sensible[86].

B. Le régime juridique: interdiction de principe assortie d'exceptions

Comme nous l'avons déjà évoqué ci-dessus, l'option choisie par le législateur consiste en une interdiction de principe de traiter les données sensibles, interdiction assortie de treize exceptions, énumérées de manière limitative aux §§ 2 et 3 de l'article 6. Ces exceptions peuvent être regroupées en trois catégories, à savoir les exceptions générales, les exceptions pour raisons d'intérêt public, et les autorisations spéciales du Roi. A cela s'ajoute une catégorie particulière, à savoir celle de la dispensation de soins.

1) Les exceptions générales

La première exception mentionnée par la loi est celle du **consentement écrit de la personne concernée**. Rappelons que pareille expression de volonté doit être libre, spécifique, informée et susceptible d'être retirée à tout moment. L'arrêté royal d'exécution précise en outre, en son article 26, que si le traitement est exclusivement autorisé par le consentement de la personne concernée, des informations complémentaires doivent lui être fournies. De plus, la loi prévoit la possibilité pour le Roi de déterminer certains cas dans lesquels l'interdiction de traitement ne peut être levée par consentement, ce que l'arrêté royal exécute en son article 27. Il s'agit des cas dans lesquels le consentement de la personne concernée, au vu des circonstances particulières, serait davantage une illusion. Ainsi, lorsque le traitement est autorisé exclusivement sur base du consentement, et que le responsable du traitement est l'employeur actuel ou potentiel de la personne concernée, ou que celle-ci se trouve dans une position dépendante vis-à-vis du responsable du traitement, le traitement sera interdit. L'article poursuit cependant en énonçant que l'interdiction sera levée si le traitement vise à procurer un avantage à la personne concernée. Cet avantage doit non seulement être voulu, mais également effectivement présent, ce qui exclut les avantages apparents. Il peut consister par exemple en paiement d'allocations syndicales, ou en la mise à disposition d'une chapelle en fonction du nombre de pratiquants au sein des membres du

[85] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 386.
[86] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 139.

personnel. Notons que cette disposition "n'empêche nullement l'employeur de traiter des données sensibles relatives à ses employés en se fondant sur d'autres critères que le consentement de la personne concernée, par exemple lorsque le traitement est nécessaire afin d'exécuter des obligations spécifiques en matière de droit du travail"[87]. Selon certains auteurs toutefois, la "solution proposée dans l'arrêté royal soulève une double critique: non seulement on admet comme valable un consentement qui ne peut être reconnu comme libre, mais encore, aucune appréciation de l'avantage promis par l'employeur n'intervient"[88]. En effet, "'un consentement exprimé par l'employé ou le candidat à l'emploi dans les mêmes conditions de dépendance sera considéré comme valable et légitimant le traitement des données s'il y a un avantage à la clé"[89]. Si la Commission de la protection de la vie privée règle le problème du consentement libre par un consentement éclairé – proposant d'exiger un consentement écrit spécial après information – elle est toutefois en contradiction avec la directive européenne, l'information supplémentaire ne dégageant pas les employés de leur état de dépendance. Il semble que le raisonnement du gouvernement se soit situé davantage au niveau de la condition de finalité légitime du traitement, estimant que si le traitement vise l'octroi d'un avantage, l'atteinte est compensée et ne présente plus de caractère disproportionné. Cependant, tout avantage, si minime ou illusoire soit-il, lève l'illégitimité du traitement, sans aucune considération de la nature de cet avantage, ce qui peut porter à critique.

Une seconde exception générale est celle de l'exécution des obligations et des droits spécifiques du responsable du traitement en matière de **droit du travail**: lorsque le traitement est nécessaire à pareille exécution, l'interdiction de principe est levée. Cette disposition devant être interprétée de manière restrictive, l'on exige que les droits et obligations proviennent de règles de droit qui réglementent les relations de travail, sans se préoccuper de savoir si ces relations concernent le secteur privé ou public[90]. Cette exception se justifie par le fait que de nombreuses normes de droit du travail rendent le traitement de données à caractère personnel nécessaire – comme par exemple la réglementation du congé politique et syndical, ou en matière d'élections du conseil d'entreprise. Il ne serait donc pas raisonnable d'exiger à chaque fois le consentement de la personne concernée.

Les **intérêts vitaux** de la personne concernée ou d'un tiers justifient également la levée de l'interdiction de traitement des données sensibles. Cette exception peut être invoquée lorsque le traitement est nécessaire à la défense de ces intérêts vitaux, ce qui exige un état de nécessité. Autrement dit, la vie de la personne concernée ou d'une autre personne doit être en jeu. S'agissant des intérêts d'un tiers, ceux-ci ne peuvent valoir pour l'invocation de l'exception que si la personne concernée se trouve d'ans l'incapacité physique ou juridique de donner son consentement.

Une quatrième exception générale concerne le traitement "effectué dans le cadre des **activités légitimes d'une fondation, une association ou tout autre organisme à**

[87] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 459.
[88] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 460.
[89] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 459.
[90] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 146; et Rapport au Roi par A.R. n° 14 du 22 mai 1996, *M.B.* 30 mai 1996, 14520.

but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées" (art. 6, § 1er, d)). Toute association n'est pas concernée, la permission de traitement n'étant reconnue qu'au responsable ayant une certaine qualité, comme par exemple celle de parti politique, de syndicat, ou encore de paroisse. En outre, le traitement doit porter exclusivement sur les données des membres de l'association, ces données ne pouvant être communiquées à des tiers. L'idée à la base de cette disposition réside dans la considération que de telles associations effectuent pareils traitements dans l'intérêt de leurs membres, sans vouloir en tirer un quelconque profit[91].

Le traitement sera en outre autorisé lorsqu'il porte sur des **données manifestement rendues publiques** par la personne concernée. Cela se limite aux cas dans lesquels la personne concernée a véritablement l'intention de rendre ces données publiques, et ne concerne que les données rendues publiques par la personne concernée elle-même[92].

Enfin, l'interdiction est levée lorsque le traitement est nécessaire à la constatation, l'exercice ou la défense d'un **droit en justice**.

2) *Les exceptions pour raison d'intérêt public*

La directive européenne permet aux Etats membres de prévoir d'autres dérogations à l'interdiction de principe, et ce pour des raisons d'intérêt général. Selon le considérant 34 de l'instrument européen, de telles raisons peuvent concerner les domaines de la santé publique et de la protection sociale – "particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie"[93] (…) –, de la recherche scientifique et des statistiques publiques. La loi reprend ces trois domaines, tout en prévoyant une disposition plus générale, permettant les traitements de données à caractère personnel lorsqu'ils sont "permis par une loi, un décret ou une ordonnance pour un autre **motif important d'intérêt public**" (art. 6, § 1er, l)). Il convient cependant d'analyser cette disposition au regard de l'article 8, § 2 de la Convention européenne des droits de l'homme, qui indique, outre l'exigence d'une base légale et de la nécessité pour une société démocratique, les seuls buts admissibles pour justifier une ingérence par l'autorité publique dans la vie privée des citoyens[94].

---

[91] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 148.
[92] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 149.
[93] Exposé des motifs, p. 35.
[94] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 387. L'article 8.2 de la Convention européenne des droits de l'Homme énonce en effet: "Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit [le droit au respect de la vie privée et familiale] que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui".

En ce qui concerne l'exception tenant au domaine de la **sécurité sociale**, le traitement sera autorisé s'il est "nécessaire à la réalisation d'une finalité fixée par ou en vertu de la loi, en vue de l'application de la sécurité sociale" (art. 6, § 1er, h)). Cette exception se limite aux institutions de sécurité sociale, telles que décrites aux articles 1 et 2, al. 1er, 2° de la loi du 15 janvier 1990 créant et organisant la Banque carrefour de la sécurité sociale[95]. Elle a été introduite dans le but d'éviter les contestations à propos des traitements, par les institutions de sécurité sociale, de données relatives à l'appartenance des assurés à une caisse d'assurance-maladie, au nom du fait que la conviction idéologique de la personne concernée pourrait en être déduite. Cette exception fait toutefois l'objet de critiques, certains auteurs jugeant le critère de nécessité non convainquant. En effet, "le traitement peut être techniquement nécessaire à la réalisation d'une finalité légale – par exemple une gestion plus rationnelle du système – tout en impliquant une ingérence disproportionnée dans les droits et libertés individuelles"[96]. Les auteurs déplorent l'absence de garanties spécifiques légitimant la levée de l'interdiction au sein de la loi, de telles garanties étant par ailleurs imposées par la directive européenne. En outre, le Roi, dans l'exposé des motifs, se réfère à la directive européenne pour fonder l'exception en matière de sécurité sociale, l'instrument européen permettant des dérogations au nom d'un intérêt public important[97]. Les auteurs estiment toutefois qu'il "étend cependant indûment la portée du considérant. Ce dernier n'identifie pas automatiquement les domaines de la santé publique et de la protection sociale comme porteurs d'un motif important d'intérêt public permettant une dérogation générale à l'interdiction de traitement des données sensibles. Il ne vise du reste pas une dérogation générale à l'interdiction de traitement de toutes les données sensibles visées par la disposition mais de certaines catégories de données sensibles. Ce considérant invite plutôt à réfléchir sur l'existence de motifs d'intérêt public importants dans certains domaines – par exemple le domaine de la sécurité sociale – qui permettrait certaines dérogations spécifiques, par exemple en cas de collecte de données sensibles lors de demandes de prestations et de services dans le régime d'assurance maladie. La disposition commentée ne s'embarrasse quant à elle d'aucune nuance: l'application de la sécurité sociale y est considérée comme étant en elle-même le motif d'intérêt public important. On peut en outre se demander pourquoi l'application de la sécurité sociale se voit ainsi privilégiée par rapport à l'application du régime fiscal, du régime linguistique, de la matière de l'enseignement, etc."[98].

---

[95] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 151.

[96] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 387.

[97] Considérant 34 de la directive: "les Etats membres doivent également être autorisés à déroger à l'interdiction de traiter des catégories de données sensibles lorsqu'un motif d'intérêt public important le justifie dans des domaines tels que la santé publique et la protection sociale – particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie (…)".

[98] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 387.

S'agissant de la **statistique publique**, le traitement de données à caractère personnel est autorisé s'il est effectué en exécution de la loi du 4 juillet 1962 concernant la statistique publique[99].

Enfin, les traitements nécessaires à des **recherches scientifiques** ne sont autorisés qu'aux conditions fixées par le Roi. L'arrêté royal d'exécution ne traitant pas de la recherche scientifique en particulier, c'est aux conditions de l'article 25 AR, examinées ci-dessus, qu'il convient de soumettre ce type de traitement.

3) Exception dans le cadre de la dispensation de soins

L'article 6, § 1er, j) énonce que sera autorisé le "traitement nécessaire aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée" à condition que le traitement soit "effectué sous la surveillance d'un professionnel des soins de santé". Quatre finalités sont clairement énoncées, cette exception étant soumise à la surveillance d'un professionnel de santé pour pouvoir être invoquée.

4) Autorisations spéciales par arrêté royal

Enfin, la loi prévoit deux cas dans lesquels le traitement de données à caractère personnel pourra être autorisé par le Roi, à savoir: "lorsque le traitement est effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la **défense et la promotion des droits de l'homme et des libertés fondamentales**, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par le Roi, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée" (art. 6, § 1er, k)); et dans le cas de traitements effectués par des organismes ayant pour finalité d'encadrer les personnes dont le comportement sexuel peut être qualifié d'infraction (art. 6, § 3). Plusieurs conditions doivent être remplies pour obtenir cette autorisation. Le traitement ne peut porter que sur les données relatives à la vie sexuelle des personnes visées; il doit être effectué par une association dotée de la personnalité juridique ou d'utilité publique; qui doit avoir un objet statutaire principal déterminé – à savoir **l'évaluation, la guidance et le traitement des personnes dont le comportement sexuel peut être qualifié d'infraction** –; qui doit être reconnue et subsidiée par l'autorité compétente pour ce faire; et qui doit avoir reçu une autorisation particulière par arrêté royal.

§ 4. – Le traitement des données relatives à la santé

Si la directive européenne ne traite pas les données relatives à la santé comme une catégorie particulière de données à caractère personnel, mais seulement comme une des catégories de données sensibles, la loi belge leur réserve un article particulier. Le régime établi est toutefois similaire à celui auquel sont soumises les données dites sensibles, à

[99] L. Du 4 juillet 1962 relative à la statistique publique, *M.B.*, 20 juillet 1962, http://www.moniteur.be.

savoir celui d'une interdiction de principe assortie d'exceptions. Notons qu'en plus des conditions établies à l'article 25 de l'arrêté royal, le traitement de pareilles données est soumis au respect de conditions supplémentaires, établies dans la loi elle-même.

A. Que recouvre la notion de données relatives à la santé?

Alors que la notion de données sensibles est relativement large grâce au critère de la "révélation" de l'information sensible, la notion de données relatives à la santé ne s'étend qu'aux données qui concernent la santé, qui s'y rapportent directement. Ainsi, demeurent exclues de l'application de l'article 7 de la loi, les données qui ne se rapportent pas à la santé, mais dont de l'information relative à la santé peut être déduite, comme par exemple une photo d'une personne handicapée. Sont donc actuellement considérées comme données relatives à la santé toutes les données à caractère personnel qui concernent l'état de santé physique ou psychique, passé, actuel ou futur, de la personne concernée[100]. Cette définition exclut également les données purement administratives ou comptables relatives à l'état de santé et aux traitements[101]. Cela signifie que ne seront pas considérées comme données relatives à la santé le lieu de résidence d'une personne (dont pourrait être déduite la proximité avec un hôpital psychiatrique, par exemple), ni l'indication qu'une personne possède un dossier auprès d'une institution de sécurité sociale comme le Fonds pour les maladies professionnelles, ou l'INAMI. Ne consiste pas non plus en une donnée relative à la santé le degré d'incapacité de travail économique. Par contre, consisteront en de telles données les dossiers médicaux qui motivent le degré d'incapacité de travail médicale, et les demandes de remboursement de services ou prestations médicaux[102].

La notion de santé est à comprendre dans un sens large, au nom du fait que des personnes non malades peuvent s'adresser au système de santé. Ainsi, il ne s'agit pas uniquement des données médicales *stricto sensu* mais également d'autres données à caractère personnelle relatives à la santé, comme par exemple les résultats de tests psychologiques, les comptes rendus de séances psychothérapeutiques, ou encore les rapports des travailleurs sociaux.

B. Le régime juridique: interdiction de principe assortie d'exceptions

Si le traitement des données à caractère personnel relatives à la santé est en principe interdit, il est toutefois autorisé dans 11 cas, semblables aux exceptions en matière de données sensibles, mais quelque peu différents cependant. Ces dérogations peuvent être regroupées en deux catégories – exceptions générales et exceptions pour motif d'intérêt général –, auxquelles s'ajoute l'exception en matière de dispensation de soins.

---

[100] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 154.
[101] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Commentaire des articles, *Doc. Parl.,* Ch. repr., sess. ord.1990-1991, n° 47K1610001 du 6 mai 1991, p. 13, http://www.lachambre.be.
[102] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 155.

Notons que certains auteurs estiment, à juste titre semble-t-il, qu'en termes de technique législative, il aurait été peut-être plus approprié non pas d'interdire le traitement, mais de prévoir un ensemble de conditions nettement plus strictes moyennant le respect desquelles les données relatives à la santé pouvaient être traitées"[103]. En effet, à quoi bon prévoir une interdiction si c'est pour l'affaiblir de tant d'exceptions? Ne serait-il pas plus judicieux d'autoriser le traitement de données relatives à la santé tout en le soumettant à de strictes conditions?

1) Les exceptions générales

L'on retrouve tout d'abord au sein de cette catégorie, les traitements auxquels la personne concernée a consenti par écrit, de manière libre, spécifique et informée. A ce sujet, "le groupe de travail [européen] «Article 29» est d'avis que lorsque la situation médicale exige nécessairement et inévitablement que le praticien de santé traite des données à caractère personnel dans un système de DME, il est trompeur que ce praticien cherche à légitimer ce traitement par le consentement. Le recours au consentement doit être limité aux cas où la personne concernée est véritablement libre de son choix et a la possibilité de retirer ultérieurement son consentement sans subir de préjudice"[104]. Le **consentement** doit en outre pouvoir être retiré à tout moment, sans que la personne concernée n'ait à justifier d'un motif pour obliger le responsable à mettre fin au traitement de ses données[105]. Les articles 26 et 27 de l'arrêté royal d'exécution, examinés ci-dessus, et concernant les cas dans lesquels l'interdiction ne peut être levée par le seul consentement, en raison de la situation de dépendance dans laquelle se trouve la personne concernée vis-à-vis du responsable du traitement, sont également d'application ici. Notons que cette exception parait fort abstraite, les personnes concernées étant rarement au courant de tous les traitements réalisés sur base de leurs données, et donc en mesure d'y consentir. Le groupe de travail "article 29" l'a d'ailleurs fait remarquer en ces termes: "le consentement était parfois difficile à obtenir en raison de problèmes pratiques, notamment en l'absence de contact direct entre le responsable du traitement et les personnes concernées". Les experts ajoutent cependant que "quelles que puissent être ces difficultés, le responsable du traitement doit pouvoir prouver en toutes circonstances, d'une part, qu'il a obtenu le consentement explicite de chaque personne concernée et, d'autre part, que ce consentement a été donné sur la base d'informations suffisamment précises"[106].

---

[103] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 331.

[104] Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007 par le Groupe de travail "ARTICLE 29" sur la protection des données, Commission européenne, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf, p. 9.

[105] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 335.

[106] Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007 par le Groupe de travail "ARTICLE 29" sur la protection des données, Commission européenne, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf, p. 10.

Le traitement de données à caractère personnel relatives à la santé sera également justifié par la nécessité d'exécuter les droits et obligations spécifiques incombant au responsable du traitement en matière de **droit du travail**. C'est le cas par exemple de l'application de la réglementation en matière de suspension du contrat de travail pour cause de grossesse ou d'allaitement maternel[107].

Les **intérêts vitaux** de la personne concernée ou d'un tiers, aux mêmes conditions qu'en matière de données sensibles, permettent de traiter les données relatives à la santé tout comme c'est le cas pour les **données manifestement rendues publiques** par la personne concernée elle-même, avec l'intention de le faire. Selon le groupe de travail "article 29", les intérêts vitaux de la personne concernée ou de tiers, sont à interpréter de la sorte: "le traitement des données doit concerner des intérêts personnels essentiels de la personne concernée ou d'une autre personne et doit – dans le contexte médical – être nécessaire à un traitement dont dépend la vie dans une situation où la personne concernée n'est pas en mesure de manifester sa volonté. Par conséquent, cette dérogation ne peut s'appliquer qu'à un nombre limité de traitements médicaux et ne peut en aucun cas être utilisée pour justifier le traitement de données médicales à caractère personnel à d'autres fins que les soins à dispenser à la personne concernée: par exemple, pour mener des recherches médicales générales qui ne donneront pas de résultats avant un certain temps"[108].

Si l'exception tenant à la constatation, l'exercice ou la défense d'un **droit en justice** existe également en ce qui concerne les données sensibles, en revanche l'exception relative à la **prévention d'un danger concret ou à la répression d'une infraction pénale déterminée** est nouvelle ici (art. 7, § 1er, g)). Cette exception est basée sur l'article 4.3 a) ii de la Recommandation n° R(97) 5 du Conseil de l'Europe relative à la protection des données médicales[109], et concerne le traitement des données génétiques[110]. Il convient de préciser que le danger visé doit présenter un caractère concret, et ne peut consister en mesures de politiques générales visant un objectif collectif de prévention. De la même manière, "pour ce qui est de la répression d'une infraction déterminée, il doit s'agir d'une enquête pénale particulière et non d'analyses comparatives entre diverses affaires"[111].

---

[107] Rapport au Roi par AR n° 14 du 22 mai 1996, *M.B.,* 30 mai 1996, 14520.

[108] Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007 par le Groupe de travail "ARTICLE 29" sur la protection des données, Commission européenne, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf, p. 10.

[109] Recommandation n° R(97) 5 du 13 février1997 du Comité des Ministres du Conseil de l'Europe aux Etats membres relative à la protection des données médicales, http://www.coe.int.

[110] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 160. La Recommandation spécifie que le traitement de données génétiques pour les nécessités d'une procédure judiciaire ou d'une enquête pénale doit faire l'objet d'une loi spécifique offrant les garanties adéquates. La Belgique s'est conformée à cette recommandation en adoptant la loi du 22 mars 1999 relative à la procédure d'identification par analyse ADN dans les affaires pénales (*M.B.,* 20 mai 1999, 17547).

[111] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 343.

2) *Les exceptions pour raison d'intérêt général*

Au rang des exceptions justifiées par un motif d'intérêt général, l'on retrouve les domaines de la **sécurité sociale** et de la **recherche scientifique** – l'objectif étant de concilier deux impératifs fondamentaux, à savoir l'évolution de la recherche et le droit de la personne concernée à voir ses droits et libertés fondamentaux, et en particulier sa vie privée, protégés[112] –, tout comme la disposition générale concernant les **autres motifs importants d'intérêt public** au nom desquels une loi, un décret ou une ordonnance rend obligatoire le traitement de données à caractère personnel relatives à la santé. Rappelons que la directive européenne mentionne, en son considérant 34, la santé publique et la sécurité sociale comme étant des domaines dans lesquels des cas d'intérêt public important sont susceptibles de se manifester. L'exposé des motifs de la loi belge cite comme exemple la cause du décès lors de l'enregistrement de celui-ci dans les registres de l'Etat[113]. Notons qu'en tout état de cause, "le fondement législatif devrait être suffisamment précis et impératif pour que le caractère obligatoire du traitement ne puisse être mis en doute"[114]. Un autre exemple de motif d'intérêt public important figure dans une proposition de règlement européen relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, dont les motivations invoquent que "les actions et stratégies politiques communautaires et nationales dans les domaines de la santé publique et de la santé et de la sécurité au travail représentent un intérêt public important"[115]. Cela ne se justifie qu'à la condition que des "garanties appropriées pour la

---

[112] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 337.

[113] Exposé des motifs, p. 40.

[114] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 343.

[115] Proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, 7 février 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007PC0046:FR:HTML: "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 et le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 le rendant applicable aux institutions et organes communautaires autorisent le traitement des données personnelles relatives à la santé pour des motifs d'intérêt public importants et sous réserve de garanties appropriées. Les actions et stratégies politiques communautaires et nationales dans les domaines de la santé publique et de la santé et de la sécurité au travail représentent un intérêt public important et les dispositions des règlements (CE) n° 322/97 et (Euratom, CEE) n° 1588/90 du 11 juin 1990 relatif à la transmission à l'Office statistique des Communautés européennes (Eurostat) d'informations statistiques couvertes par le secret prévoient des garanties appropriées pour la protection des individus dans le cas de la production de statistiques communautaires sur la santé publique et sur la santé et la sécurité au travail". Voy. également le considérant n° 12: "Les exigences statistiques résultant de l'action communautaire dans le domaine de la santé publique, des stratégies nationales pour le développement de soins de santé de qualité, accessibles et durables et de la stratégie communautaire de santé et de sécurité au travail, ainsi que les exigences liées aux indicateurs structurels, aux indicateurs de développement durable, aux indicateurs de santé de la Communauté européenne et à d'autres ensembles d'indicateurs qu'il convient de développer pour assurer le suivi des actions et stratégies politiques communautaires et nationales dans les domaines de la santé publique et de la santé et de la sécurité au travail, représentent un intérêt public important".

protection des individus dans le cas de la production de statistiques communautaires sur la santé publique et sur la santé et la sécurité au travail" soient prévues, ce qui en l'espèce est le cas selon la Commission européenne[116]. Ces garanties, énoncées au chapitre V du règlement n° 322/97 relatif à la statistique communautaire[117], ce chapitre étant relatif au secret statistique, tiennent au caractère confidentiel des données permettant une identification directe ou indirecte, les agents utilisant ces données étant tenus au respect du secret statistique qui s'y attache. La transmission de ces données confidentielles entre autorités nationales et communautaire n'est admise que dans la mesure où elle est nécessaire à la production de statistiques communautaires. Toute transmission ultérieure doit faire l'objet d'une autorisation expresse de la part de l'autorité nationale qui a collecté les données. Une autre garantie tient à l'utilisation des données, qui se limite exclusivement à des fins statistiques, sauf consentement exprès et sans équivoque des personnes concernées. En outre, l'accès à ces données est, tout comme la transmission, limité à ce qui est nécessaire pour la production de statistiques communautaires. Les Etats membres et la Commission décident des modalités pratiques, des limites et des conditions nécessaires pour que l'accès soit effectif. L'accès aux données à des fins scientifiques peut-être accordé à condition qu'un niveau de protection suffisant soit assuré. Enfin, l'article 18.1 du règlement prévoit que "les mesures réglementaires, administratives, techniques et organisationnelles nécessaires sont prises aux niveaux national et communautaire pour assurer la protection physique et logique des données confidentielles et pour éviter tout risque de divulgation illicite ou d'utilisation à des fins autres que statistiques lors de la diffusion des statistiques communautaires". L'on voit que la description de ces garanties reste fort vague, ne conférant qu'un faible caractère de concrétisation aux mesures destinées à garantir le respect de la vie privée.

Si la statistique publique n'est pas présente au sein de l'article 7, une nouvelle raison d'intérêt général y figure, à savoir celle de la promotion et la protection de la **santé publique**, incluant le dépistage (art. 7, § 1er, d)).

3) *Exception dans le cadre de dispensation de soins*

L'article 7, § 1er, j) reprend mot pour mot le point j) de l'article 6, autorisant de la sorte les traitements de données relatives à la santé, lorsqu'ils sont nécessaires aux fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements, et de la gestion des services de santé. Les mêmes conditions sont prévues, à savoir l'exigence d'agir dans l'intérêt de la personne concernée, et sous surveillance d'un professionnel de la santé.

Cette exception trouve sa source dans l'article 8, § 3, de la directive 95/46/CE qui, selon le groupe de travail "article 29", "couvre uniquement le traitement de données à

---

[116] En effet, selon le texte de la même proposition de règlement, "les dispositions des règlements (CE) n° 322/97 [du 17 février 1997 relatif à la statistique communautaire] et (Euratom, CEE) n° 1588/90 du 11 juin 1990 relatif à la transmission à l'Office statistique des Communautés européennes (Eurostat) d'informations statistiques couvertes par le secret prévoient des garanties appropriées pour la protection des individus dans le cas de la production de statistiques communautaires sur la santé publique et sur la santé et la sécurité au travail.

[117] Règlement (CE) n° 322/97 du conseil du 17 février 1997 relatif à la statistique communautaire, art. 13 à 18, *J.O.,* n° L 052 du 22 février 1997, pp. 0001/0007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997R0322:FR:HTML.

caractère personnel dans le but spécifique de fournir des services de santé à caractère préventif, diagnostique, thérapeutique ou de postcure et de gérer ces services de soins de santé, par exemple pour la facturation, la comptabilité ou les statistiques. Elle ne couvre pas un traitement ultérieur non nécessaire à la fourniture directe de ces services, notamment l'utilisation des données pour la recherche médicale, le remboursement ultérieur des frais par un régime d'assurance maladie ou le recouvrement de créances. Échappent également au champ d'application de l'article 8, paragraphe 3, d'autres opérations de traitement de données dans des domaines tels que la santé publique et la protection sociale, visant notamment à assurer la qualité et la rentabilité des procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance maladie, puisque ces opérations sont mentionnées au considérant 34 de la directive en tant qu'exemples d'invocation de l'article 8, paragraphe 4"[118], lequel concerne les motifs d'intérêt public importants, examinés ci-dessus. A cette première condition tenant à la finalité du traitement, s'ajoute, selon le régime de la directive tel qu'analysé par le groupe de travail "article 29", celle de la stricte nécessité – dépassant la simple utilité –, ainsi que celle de la confidentialité – le traitement devant être réalisé par un professionnel de la santé soumis au secret professionnel, ou toute autre personne tenue par une obligation de secret équivalente. S'agissant du dossier médical électronique (DME) – ou dossier patient informatisé –, " le groupe de travail «Article 29» n'est pas convaincu que, même si l'article 8, paragraphe 3, est utilisé pour justifier le traitement des données, l'obligation de secret professionnel assure à elle seule une protection suffisante en cas de DME. De nouveaux risques appellent des garanties supplémentaires, voire nouvelles, par rapport à celles qui sont requises par l'article 8, paragraphe 3, afin d'assurer une protection suffisante des données à caractère personnel dans un contexte de DME"[119]. En effet, les risques sont plus élevés dans le cas du DME, "puisque l'un des objectifs du DME est de mettre les professionnels qui n'ont pas participé au traitement médical précédent consigné dans un fichier médical en mesure d'accéder aux documents médicaux à des fins de traitement"[120]. Les conditions prévues par la loi belge, celle-ci étant une transposition de la directive européenne, semblent donc être quelque peu dépassées et dès lors insuffisantes face aux progrès technologiques et au développement d'internet.

C. Les garanties supplémentaires

Des garanties supplémentaires encadrent le traitement de données à caractère personnel relatives à la santé, ces garanties figurant au sein de la loi elle-même, et

[118] Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007 par le Groupe de travail "ARTICLE 29" sur la protection des données, Commission européenne, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf, p. 11.
[119] Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007 par le Groupe de travail "ARTICLE 29" sur la protection des données, Commission européenne, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf, p. 13.
[120] *Ibid.*

s'ajoutant aux conditions fixées par l'arrêté royal d'exécution en son article 5 (auquel renvoie l'article 7, § 3 de la loi). Ces garanties sont au nombre de trois.

Tout d'abord, pareil traitement ne peut être effectué, selon l'article 7, § 4 que **sous la surveillance d'un professionnel des soins de santé**, cette notion étant à interpréter de manière large, l'expression "professionnel des soins de santé" visant toutes les personnes qui procurent des soins à d'autres personnes dans l'exercice de leur métier[121]. L'exposé des motifs vise également les personnes travaillant pour le compte de professionnels de soins de santé, justifiant cette extension en invoquant l'article 8.3 de la directive qui vise "tant le professionnel des soins de la santé soumis par le droit national au secret professionnel qu'à d'autres personnes soumises à une obligation de secret équivalente"[122]. Ce professionnel de la santé doit être tenu au secret professionnel, la loi créant une obligation de confidentialité spécifique, sans préjudice des autres obligations de secret professionnel existantes, comme celle établie par le Code pénal. Ce secret professionnel spécifiquement créé est sanctionné pénalement à l'article 39, 3° de la loi, cette sanction pénale étant donc distincte de l'article 458 du Code pénal. L'exigence de la surveillance d'un professionnel de santé n'est pas une obligation absolue, n'étant pas imposée dans deux cas, à savoir celui du traitement auquel la personne concernée a consenti par écrit, et celui du traitement nécessaire à la prévention d'un danger actuel ou à la répression d'une infraction pénale déterminée. Il est important de préciser que l'intervention d'un professionnel de santé n'est jamais une justification indépendante du traitement de données relatives à la santé. Il ne s'agit que d'une condition complémentaire à respecter, en plus de la nécessité de pouvoir invoquer une base légale, à savoir un des cas d'exceptions prévus à l'article 7 de la loi[123].

En outre, les données relatives à la santé ne peuvent être **collectées qu'auprès de la personne concernée** elle-même (art. 7, § 5), cette exigence visant à éviter que de telles données soient récoltées auprès de nombreuses sources sans que la personne concernée n'opère aucun contrôle[124]. L'article prévoit toutefois deux possibilités de déroger à cette règle, à condition que les autres garanties soient respectées: lorsque la collecte auprès de tiers soit nécessaire aux fins du traitement – exception qui, selon certains auteurs, "risque de vider le principe de toute portée"[125] –, et lorsque la personne concernée ne soit pas en mesure de fournir les données elle-même – en cas d'état comateux, par exemple.

Enfin, une dernière garantie est prévue à l'article 10, § 2, traitant du **droit d'accès** de la personne concernée, ayant pour corollaire une obligation de communication dans le chef du responsable du traitement – et dont nous traiterons dans la section consacrée aux droits de la personne concernée. En effet, une procédure particulière est prévue lorsque le traitement porte sur des données relatives à la santé. Ainsi, la personne concernée – et elle seule – qui apporte la preuve de son identité peut, soit directement, soit indirectement – c'est-à-dire via l'intermédiaire d'un professionnel de santé –, se faire communiquer

---

[121] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 163.
[122] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 388. Exposé des motifs, p. 39.
[123] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 164.
[124] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 165.
[125] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 333.

toutes les données qui sont traitées et qui concernent sa santé. La communication pourra toutefois être différée en cas de traitement aux fins de recherches médico-scientifiques, jusqu'à l'achèvement de celles-ci, moyennant le respect de plusieurs conditions. Il doit être manifeste qu'aucun risque d'atteinte à la vie privée de la personne concernée n'est présent; les données ne peuvent être utilisées pour prendre des mesures à l'égard d'une personne concernée individuelle; la communication immédiate des données doit être susceptible de nuire gravement à la recherche; et la personne concernée doit avoir préalablement donné son autorisation écrite au responsable du traitement de traiter des données la concernant aux fins de recherches médico-scientifiques, et de différer la communication de celles-ci. Il convient de préciser qu'il ne s'agit pas d'une dérogation à l'obligation de communiquer les données, mais bien simplement d'une possibilité de différer celle-ci. Cette faculté "trouve son fondement dans la nécessité de pouvoir réaliser des expérimentations médicales et en particulier des essais cliniques de médicaments en "double aveugle" qui permettent notamment de mesurer l'effet placebo d'un médicament"[126].

§ 5. – Le traitement des données judiciaires

Cette catégorie de données nous semble moins pertinente en matière de santé publique, raison pour laquelle nous ne l'envisagerons que brièvement. La loi du 8 décembre 1992 interdit, en son article 8, le traitement des données à caractère personnel "relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté". C'est donc une notion relativement large que recouvre le concept de donnée judiciaire, incluant non seulement les sentences et arrêts des cours et tribunaux civils, commerciaux, sociaux et administratifs (ce dernier cas visant principalement le Conseil d'Etat), mais également toutes les données à caractère personnel relatives aux sanctions administratives, aux mesures de sécurité – visant les mesures relatives aux étrangers, à la protection de la jeunesse, aux malades mentaux, etc. – et enfin les données de droit pénal, celles-ci allant de la suspicion à la condamnation, en passant par les poursuites.

La doctrine opère un certain nombre de distinctions au sein de ces données dites judiciaires, certains critères intervenant dans l'application des exceptions à l'interdiction de principe. Ainsi, certaines données judiciaires revêtent un caractère public, de par la publication d'une sentence ou d'un arrêt, ou de par le prescrit légal de publication. Un autre critère distingue les données judiciaires objectives des données judiciaires subjectives. Si les premières répondent à une réalité établie, et reposent sur une source possédant un degré raisonnable de fiabilité et d'objectivité; les secondes sont le résultat d'une qualification, d'une interprétation ou d'une appréciation par le responsable du traitement, cette catégorie visant plus particulièrement les suspicions et poursuites relatives aux infractions. Enfin, il convient de différencier les données selon la personne

[126] M.-H. BOULANGER, S. CALLENS et St. BRILLON, "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 345.

auxquelles elles se rapportent, celle-ci pouvant être un client ou un tiers, avec lequel le responsable du traitement a une relation contractuelle ou légale[127].

L'article 8 établit un régime juridique semblable à celui des articles 6 et 7, si ce n'est que les exceptions à l'interdiction de principe de traiter ce type de données sont relativement limitées. L'on retrouve le cas des traitements nécessaires à la réalisation de finalités fixées par la loi, ainsi que l'exception en matière de recherche scientifique. Les autres exceptions sont plus spécifiques au domaine judiciaire, le traitement des données à caractère personnel judiciaires étant autorisé lorsqu'il est nécessaire à l'exercice des tâches d'une autorité publique ou d'un officier ministériel au sens du Code judiciaire et qu'il est exécuté sous le contrôle de ceux-ci, lorsqu'il est nécessaire à la gestion d'autres contentieux de personnes physiques ou morales, et enfin lorsqu'il est exécuté par des avocats ou d'autres conseils juridiques – à savoir des notaires, huissiers de justice, préposés de compagnies d'assurances ou d'organisations syndicales représentatives – pour autant que la défense de leur client l'exige. C'est donc le bon fonctionnement du système judiciaire et la défense d'autres personnes dans d'autres contentieux qui justifient ces exceptions. Notons que le paragraphe 3 de l'article 8 soumet les responsables des traitements exceptionnels de données judiciaires à une obligation de secret professionnel, cette dernière étant pénalement sanctionnée dans la loi elle-même, et ne portant pas atteinte aux autres obligations de confidentialités existantes[128].

Section II. – Les droits de la personne concernée et les obligations du responsable du traitement

Le respect des conditions de licéité du traitement ne suffit pas à traiter des données à caractère personnel en conformité avec la loi. En effet, celle-ci reconnaît un certain nombre de droits à la personne concernée, droits qui correspondent à autant d'obligations dans le chef du responsable du traitement. Le non respect d'un de ces droits et obligations est donc source d'illégalité. La loi traite des droits de la personne concernée en son chapitre III, après avoir énoncé en son article 2 son principe général, à savoir le respect de la vie privée.

§ 1er. – Le droit à la protection des libertés et droits fondamentaux, notamment à la protection de la vie privée

En amont des droits spécifiques au traitement de données à caractère personnel, reconnus à la personne concernée, celle-ci a tout d'abord le droit de voir sa vie privée respectée et protégée. C'est l'objet même de la loi, les autres droits n'étant que des moyens visant à garantir le respect de celui-ci. L'article 2 de la loi relative à la protection de la vie privée énonce ce droit en ces termes: "Lors du traitement de données à caractère

[127] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 171.
[128] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 176-177.

personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée".

L'affirmation de ce droit comme principe général, en tout début de la loi, lui confère un rôle de fil rouge servant de guide à l'interprétation de toutes les autres dispositions: les difficultés pratiques et concrètes doivent donc être résolues à la lumière du principe du respect des droits et libertés fondamentaux, en particulier de la vie privée[129].

L'insertion de ce principe dans la loi offre au citoyen un fondement juridique pour la protection de sa vie privée, qu'il peut revendiquer[130]. Si l'effet horizontal de ce droit – à savoir l'effet qu'il opère dans les relations entre la personne concernée et le responsable du traitement (un effet vertical opérant entre une personne physique ou morale et l'Etat) – est contesté par certains en raison de la nature fondamentale du droit au respect de la vie privée, il semble que cet effet horizontal puisse néanmoins être confirmé[131].

La loi n'offre aucune définition de la vie privée, car cette notion est subjective, dépendant des opinions qui dominent dans la société et qui varient selon les groupes et les époques. Il convient donc de se référer à la notion de vie privée telle que comprise dans la Convention européenne des droits de l'homme, ainsi qu'à la doctrine et à la jurisprudence développées à ce sujet. C'est principalement la reconnaissance du droit d'autodétermination qui est au fondement de la protection de la vie privée[132].

§ 2. – Le droit à l'information

L'article 9 incarne l'exigence de transparence du traitement des données à caractère personnel, celle-ci étant une des caractéristiques principales de la loi, mise en évidence entre autres par la consécration de ce droit à l'information[133], lequel droit a pour corolaire une obligation d'information incombant au responsable du traitement. La loi concrétise ce dernier de deux manières différentes, selon que les données sont obtenues auprès de la personne concernée elle-même ou auprès de tiers. L'article 9 prévoit en outre certaines exceptions à cette obligation d'information, ainsi que les modalités de celle-ci.

A. Obtention des données auprès de la personne concernée

Il convient de bien déterminer ce que signifie l'obtention des données auprès de la personne concernée afin de définir la portée exacte de l'obligation d'information. Le terme "obtention" ne signifie pas que soient seuls visés les cas dans lesquels le

---

[129] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 182-183.

[130] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la commission de la justice par Mme Merckx-Van Goey, *Doc. Parl.*, Ch. repr., sess. exrtr. 1991-1992, n° 413/012 du 2 juillet 1992, pp. 9-10, http://www.lachambre.be.

[131] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 183-184.

[132] Pour plus de détails à propos des considérations doctrinales, voy. D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 184-187.

[133] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Rapport fait au nom de la commission de la justice par Mme Merckx-Van Goey, *Doc. Parl.*, Ch. repr., sess. exrtr. 1991-1992, n° 413/012 du 2 juillet 1992, p. 10, http://www.lachambre.be.

responsable du traitement est à l'initiative de la collecte des données. En effet, sont également inclus les cas dans lesquels la personne concernée elle-même communique spontanément des données au responsable du traitement. Il peut donc s'agir de la soumission d'un formulaire ou de coupons à compléter, d'enquêtes téléphoniques ou encore de la communication spontanée de données par la personne concernée lors d'une visite à un hôpital, par exemple[134].

Les données doivent donc être obtenues auprès de la personne concernée, qu'elles soient sollicitées ou communiquées spontanément. De plus, il doit s'agir de données à caractère personnel qui la concernent en propre, et non des données concernant d'autres personnes physiques. Enfin, et même si la loi ne le précise pas, le responsable du traitement ne sera tenu à l'obligation d'information que si les données obtenues auprès de la personne concernée et relatives à elle, feront l'objet d'un traitement automatisé ou non, ou seront enregistrées dans un fichier[135].

B. Obtention auprès de tiers

Dans de nombreux cas, les données ne seront pas obtenues auprès de la personne concernée elle-même, comme par exemple en cas d'achat ou de location de (fichiers de) données, de communication par des tiers, ou encore via des banques de données sur internet. Cela n'empêche pas que la personne concernée doive savoir ce qu'il advient de ses données et l'usage que l'on en fait, raison pour laquelle la loi prévoit également une obligation d'information dans ce cas, en son article 9, § 2.

La formulation compliquée de cette disposition étant source d'une grande incertitude dans la pratique, un avis a été demandé à la Commission de la protection de la vie privée lors des travaux préparatoires[136]. Celle-ci a donc déclaré que l'article 9, § 2 vise "toutes les situations dans lesquelles les données n'ont pas été collectées auprès de la personne concernée *pour les finalités visées* et ces finalités ne pouvaient donc pas être mentionnées lors de la collecte des données". La Commission distingue trois situations visées par cette disposition, la première étant celle du responsable du traitement qui souhaite utiliser des données à caractère personnel pour d'autres finalités que celles visées lors de la collecte ou du premier enregistrement. Tombe également sous le coup de cette disposition le responsable du traitement qui veut communiquer des données à un tiers pour d'autres finalités que celles prévues au moment de la collecte ou du premier enregistrement. Enfin, l'article 9, § 2 s'applique également au moment du premier enregistrement des données si celles-ci n'ont pas été collectées auprès de la personne concernée[137].

---

[134] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 188-189.
[135] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 190; Memorie van Toelichting, p. 44.
[136] Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, http://www.privacycommission.be.
[137] Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, http://www.privacycommission.be, p. 15.

C. Les modalités de l'information

Que les données soient récoltées auprès de la personne concernée ou de tiers, la loi impose certaines modalités quant à la communication de l'information, ayant trait au contenu de celle-ci, au moment auquel elle doit être fournie, et à la manière dont elle doit être transmise.

1) Le contenu de l'information

Il convient de distinguer différentes sortes d'informations[138]. Une première catégorie est celle de **l'information minimale**, de base, qui doit être transmise en toutes circonstances. Il s'agit du nom et de l'adresse du responsable du traitement, ainsi que des finalités de celui-ci.

Vient ensuite **l'information complémentaire**, à fournir lorsque la finalité de marketing direct est envisagée par le responsable du traitement: la personne concernée doit être informée de son droit d'opposition à un tel traitement. L'arrêté royal d'exécution offre plus de précisions quant aux modalités d'exercice de ce droit d'opposition, afin de conférer une réelle effectivité à cette disposition. Nous examinerons ces modalités au cours du paragraphe concernant le droit d'opposition.

Enfin, la loi impose au responsable du traitement de transmettre certaines **informations supplémentaires**, sauf si celles-ci ne sont "pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données" (art. 9, § 1er, d) et § 2, d)), la notion de traitement loyal faisant référence à l'exigence de transparence. Le responsable du traitement est donc en principe tenu de fournir ces informations supplémentaires, et n'en sera dispensé que lorsqu'il sera en mesure de démontrer qu'elles ne sont pas nécessaires pour garantir le caractère loyal du traitement. Ces informations tiennent notamment aux catégories de données, aux catégories de destinataires, et à l'existence d'un droit d'accès et de rectification. De plus, la loi permet au Roi d'imposer la communication d'autres informations supplémentaires en fonction du caractère spécifique du traitement, ce que l'arrêté royal exécute en ce qui concerne les traitements aux fins de marketing direct, et en matière de traitement de données sensibles ou relatives à la santé (art. 26 AR).

2) Le moment de la communication de l'information

Le moment auquel l'information doit être transmise à la personne concernée diffère selon que les données ont été obtenues auprès de celle-ci ou de tiers. En effet, si l'article 9, § 1er prévoit que l'information doit être fournie à la personne concernée au plus tard au moment où les données sont obtenues auprès d'elle – la Commission de la protection de la vie privée interprétant ces termes en ce sens que l'information a lieu en même temps que la collecte, "étant entendu que la personne concernée doit tout de même

[138] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, pp. 388-389; et D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 203-209.

garder la possibilité de ne pas communiquer les données à caractère personnel la concernant, à la lumière des informations qui lui sont fournies", sans quoi l'obligation d'information serait dépourvue de sens[139] –, tandis que selon le § 2 du même article, "l'information a lieu, au choix du responsable à qui les données ont été transférées, soit à l'enregistrement, soit si une communication à un tiers est envisagée, au plus tard lors de la première communication"[140].

Notons que l'article 30 de l'arrêté royal d'exécution prévoit que l'obligation d'information peut être reportée jusqu'au premier contact avec la personne concernée, lorsque l'information immédiate est impossible ou implique des moyens disproportionnés[141].

3) La manière de communiquer l'information

La loi n'impose aucune manière particulière de communiquer l'information, offrant ainsi de larges possibilités au responsable du traitement. L'information peut donc être transmise aussi bien oralement que par écrit, tout comme une information collective est également possible. S'il parait raisonnable d'opter pour une manière d'informer qui soit proportionnelle à la manière de collecter les données – l'information étant transmise, dans le cas d'une enquête écrite par exemple, via un texte sur le formulaire d'enquête –, il convient de prendre en considération l'importance de la communication de l'information en rapport avec les exceptions à l'obligation d'information. L'une d'elles, en effet, et comme nous le verrons ci-dessous, concerne les cas dans lesquels la personne concernée est déjà informée[142].

D. Les exceptions à l'obligation d'information

Une première catégorie d'exceptions à l'obligation d'information est une conséquence de **l'application modulée de la loi** à certaines catégories de personnes. En effet, nous avons examiné, au cours du premier chapitre de ce document, un certain nombre d'exceptions partielles au champ d'application de la loi. C'est ainsi que l'article 3 dispense de l'obligation d'information les responsables du traitement à des fins exclusivement journalistiques, littéraires ou artistiques (art. 3, § 3, b)), tout comme en sont dispensés les services de renseignements et de sécurité (art. 3, § 4), ainsi que les autorités publiques dans l'exercice de leurs tâches et police administrative et judiciaire (art. 3, § 5), et enfin le Centre européen pour enfants disparus et sexuellement exploités (art. 3, § 6).

S'ajoutent à cela des exceptions spécifiques à cette disposition, pour l'examen desquelles il convient, une fois de plus, de distinguer selon que les données ont été obtenues auprès de la personne concernée ou auprès de tiers. Dans le premier cas,

[139] Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, http://www.privacycommission.be, p 13.
[140] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 389.
[141] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 209.
[142] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 210-211.

l'article 9, § 1er prévoit que **l'information ne doit pas être fournie à la personne concernée si celle-ci est déjà informée.** Plusieurs précisions ne sont toutefois pas à négliger. Il s'agit des informations décrites à l'article 9, la personne concernée devant donc déjà être au courant de tout ce qui y est mentionné, la dispense ne pouvant être partielle[143]. De plus, le responsable du traitement doit s'assurer que la personne concernée a bien été informée. Si elle l'a été par le responsable du traitement lui-même, cela ne pose pas de problème, mais cela ne vise que les situations dans lesquelles des données à caractère personnel relatives à la personne concernée sont à nouveau obtenues par le même responsable du traitement et pour les mêmes finalités. Cela est par exemple le cas du retrait de billets de banque à un guichet automatique, du paiement électronique à une station d'essence, ou encore la transmission de chèques postaux à une banque[144]. L'on voit toute l'importance de l'information qui est dispensée lors du premier traitement: plus celle-ci est détaillée quant aux finalités possibles et futures poursuivies par le responsable du traitement, moins il sera nécessaire de fournir une information supplémentaire par la suite. Si le responsable du traitement n'a pas informé lui-même la personne concernée, il doit savoir, avec un certain degré de certitude, que celle-ci l'a été. En effet, selon la Commission de la protection de la vie privée, "l'information de la personne concernée doit être une *certitude* raisonnable dans le chef du responsable, et non une *supposition*. Ceci implique, par exemple, que les formes d'information collective dans la presse générale et apparentée n'engendrent pas toujours cette certitude"[145].

S'agissant des cas dans lesquels les données ne sont pas obtenues auprès de la personne concernée elle-même, deux exceptions complémentaires à l'obligation d'information sont prévues, le cas de la personne concernée déjà informée s'appliquant également. Il s'agit tout d'abord de **l'impossibilité de fournir l'information ou du caractère disproportionné des efforts que cela implique** (art. 9, § 2, al. 2, a)). Bien que la disposition précise que cela concerne particulièrement les traitements "aux fins de statistiques ou de recherche historique ou scientifique ou pour le dépistage motivé par la protection et la promotion de la santé publique", elle s'applique à toute situation dans laquelle l'information est impossible ou implique des efforts disproportionnés[146]. L'arrêté royal d'exécution assortit cette exception de deux conditions supplémentaires, à savoir l'information de la personne concernée à la première prise de contact que le responsable du traitement – ou le tiers à qui celui-ci a communiqué les données – a avec elle (art. 30 AR); ainsi que l'obligation de justifier l'impossibilité ou le caractère disproportionné des efforts que l'information entraine, dans la déclaration que le responsable du traitement remet à la Commission de la protection de la vie privée (art. 31 AR).

Plusieurs précisions s'imposent. S'agissant tout d'abord des traitements ultérieurs à des fins statistiques, scientifiques et historiques, l'article 28 de l'arrêté royal prévoit que "le responsable du traitement ultérieur à des fins historiques, statistiques ou scientifiques, qui traite exclusivement des données codées, est exempté de l'obligation d'information, instituée à l'article 9, § 2, de la loi, sous condition du respect des dispositions du Chapitre

[143] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 389.
[144] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 194.
[145] Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, http://www.privacycommission.be, p 14.
[146] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 198-199.

II, Section II du présent arrêté", ces conditions ayant été examiné précédemment, au cours du premier chapitre de ce document. Cette exemption ne vise cependant "que les cas où le responsable du traitement initial ou un tiers, qui n'ont pas obtenu les données directement auprès de la personne concernée, souhaitent ensuite traiter les données à des fins historiques, statistiques ou scientifiques. Il y a donc eu une information de la personne concernée au départ sur la finalité initiale, mais pas concernant cette finalité ultérieure. Cela suppose également que le traitement ultérieur ne soit pas compatible avec la finalité initiale car sinon une information sur une finalité secondaire ne serait pas nécessaire. Désormais donc, lorsqu'un responsable collecte des données pour des finalités particulières et décide ultérieurement de réaliser des statistiques à partir des données récoltées qu'il coderait pour ce faire, il ne doit pas informer la personne concernée, sauf s'il s'agit de données sensibles, médicales ou judiciaires"[147].

Ensuite, l'arrêté royal encadre cette dispense de limites, considérant que l'impossibilité ou la difficulté importante de fournir l'information ne se justifie plus lorsqu'une prise de contact est établie entre le responsable du traitement – ou le tiers à qui il communique les données – et la personne concernée. L'information devra en conséquence être transmise lors de cette première prise de contact. Il semble que l'article 30 de l'arrêté royal "vise plus particulièrement, mais non exclusivement, la prospection commerciale où des kyrielles de données à caractère personnel sont collectées par des entreprises spécialisées qui transmettent ensuite ces données à d'autres entreprises à des fins de publipostage"[148]. Notons cette question de la prise de contact soulève de nombreuses interrogations lorsqu'elle doit être appliquée dans le contexte d'internet.

Enfin, la transparence que l'article 31 de l'arrêté royal cherche à établir, en imposant la justification de l'impossibilité de transmettre l'information auprès de la Commission de la protection de la vie privée, laquelle publie la liste de ces responsables du traitement dans un registre public, n'est "qu'une transparence fort relative, dans la mesure où, de cette liste de responsables de traitements, la personne concernée ne saura pas déduire qui traite ses données ni quelles données précises sont traitées et à quelles fins"[149].

La dernière exception à l'obligation d'information, lorsque les données sont collectées auprès de tiers, peut être invoquée "lorsque l'enregistrement ou la communication des données à caractère personnel 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**" (art. 9, § 2, al. 2, b)). En exécution de cette disposition, l'article 29 de l'arrêté royal exempte de l'obligation d'information les autorités administratives chargées explicitement par la loi de rassembler et de coder les données lorsqu'elles agissent en tant qu'organisation intermédiaire, visant de la sorte des organismes tels que la Banque-carrefour ou l'I.N.S. Bien que cette disposition entraine une importante limitation aux droits de la personne concernée, elle n'est assortie d'aucune garantie particulière[150], ce qui est particulièrement regrettable, la transparence dans le secteur public étant en

[147] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 460.
[148] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 460.
[149] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 461.
[150] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 201.

conséquence mise à mal. En effet, "tout fichage, toute communication de données, nécessaire voire simplement utile pour répondre à une mission conférée en termes généraux par une norme législative ou réglementaire pourra se faire sans aucune mesure d'information des personnes concernées"[151].

§ 3. – Le droit d'accès

La loi sur la protection de la vie privée offre également à la personne concernée la possibilité d'exercer un certain contrôle sur le traitement de ses données à caractère personnel. Elle doit pouvoir vérifier que les données traitées sont effectivement adéquates, pertinentes et non excessives, que le principe de finalité est bien respecté, etc. C'est pour ce faire que l'article 10 lui confère un droit d'accès, à savoir le droit d'obtenir du responsable du traitement un certain nombre d'informations et de communications. Ce droit a pour corolaire une obligation de communication dans le chef du responsable du traitement.

Rappelons qu'une procédure particulière est prévue à l'article 10, §2, en faveur des données relatives à la santé, procédure que nous avons examinée lors de l'analyse du régime juridique auquel est soumis le traitement de ces données particulières.

A. Les conditions du droit d'accès

Toute personne ne peut justifier de ce droit, la loi précisant que la requête doit émaner de la personne concernée elle-même. Cela inclut toutefois les représentants légaux, ainsi que les personnes investies d'un mandat particulier. La personne concernée doit en outre apporter la preuve de son identité. La loi ne précisant pas comment, cette condition peut être remplie en fournissant une photocopie de la carte d'identité. En effet, si les demandes effectuées par téléphone soulèvent le problème de la preuve de l'identité des demandeurs, celles introduites par courrier électronique ne sont valables que pour autant que la signature électronique soit considérée comme juridiquement équivalente à la signature manuscrite[152].

S'ajoutent à cela des conditions tenant à des exigences de validité formelles, auxquelles doit satisfaire la requête de la personne concernée. Outre l'obligation d'introduire une demande datée et signée (art. 10, § 1er, al. 2) – les requêtes téléphoniques ou orales demeurant exclues –, l'arrêté royal d'exécution précise que la demande peut aussi bien être remise sur place qu'envoyée par la poste ou par tout autre moyen de télécommunication (art. 32 A.R.). En cas de remise de la demande sur place, un accusé de réception doit immédiatement être délivré. La demande doit en principe être remise au responsable du traitement, la possibilité étant néanmoins offerte au Roi de désigner d'autres personnes à qui la requête peut être remise. C'est ainsi que l'arrêté royal d'exécution cite non seulement le représentant en Belgique du responsable du traitement,

[151] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 461.
[152] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 461.

ses mandataires ou préposés, ainsi que le sous-traitant, ses représentant, mandataires ou préposés. Cela implique que le responsable du traitement prenne les mesures organisationnelles nécessaires pour s'assurer que la demande arrive à temps auprès de la personne compétente pour la recevoir[153]. Enfin, et contrairement au système antérieur, l'exercice du droit d'accès est gratuit, en raison du fait que la personne concernée n'a pas demandé à ce que ses données à caractère personnel soient traitées[154].

B. L'information qui doit et peut être communiquée

L'article 10, § 1er, al. 1er énumère **ce que la personne concernée a le droit d'obtenir** auprès du responsable du traitement. Il s'agit tout d'abord de savoir si ses données à caractère personnel sont ou non traitées, sans que la personne concernée ne doive spécifier dans sa demande les traitements auxquels elle fait allusion. S'il n'y a pas de traitement en cours, cela doit pouvoir être confirmé. Au contraire, s'il existe un traitement quel qu'il soit, le responsable du traitement doit le lui mentionner ainsi que lui communiquer au moins les informations relatives aux finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels elles sont communiquées.

La personne concernée a en outre le droit de se faire communiquer, "sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données" (art. 10, § 1er, al. 1er, b)). En raison de considérations pragmatiques, la possibilité est offerte au responsable du traitement de moduler et d'adapter aux circonstances du cas d'espèce la manière dont les données seront communiquées, que ce soit oralement, par écrit ou d'une autre manière[155]. La seule exigence légale tient au caractère compréhensible de l'information transmise, ainsi qu'au caractère complet de celle-ci – il s'agit de communiquer toute l'information disponible.

L'article poursuit en énonçant "la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas des décisions automatisées visées à l'article 12bis". Il s'agit des décisions produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative. Il convient toutefois de prendre en compte la protection du secret des affaires et de la propriété intellectuelle, et de maintenir un équilibre entre celle-ci et la communication de l'information à la personne concernée. Une certaine information doit être transmise, mais il ne faut pas non plus communiquer trop d'information[156].

Enfin, la personne concernée a le droit d'obtenir "un avertissement de la faculté d'exercer les recours prévus aux articles 12 et 14 et, éventuellement, de consulter le registre public prévu à l'article 18". Les recours visés concernent les droits d'opposition, de rectification et de suppression dont jouit la personne concernée à l'égard du responsable du traitement, ainsi que les recours qu'elle peut introduire en justice. Nous traiterons de ces recours dans les pages qui suivent.

---

[153] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 225.
[154] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 225.
[155] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 227.
[156] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 228.

Il convient d'examiner ici la question des **limites du droit d'accès**: ce droit est-il absolu, ou bien doit il être confronté à la considération d'autres intérêts? Il semble que l'on ne puisse conférer un caractère absolu au droit d'accès, tout d'abord en raison de la vie privée de tiers. En effet, même si la loi ne prévoit pas d'exception particulière à ce sujet, cette première limite peut se fonder sur l'article 2 de la loi, lequel consacre le droit au respect de la vie privée de toute personne lors du traitement de données à caractère personnel la concernant. C'est au même titre qu'une seconde limitation au droit d'accès intervient, à savoir celle de la protection des (autres) droits et libertés fondamentaux de toute personne. Enfin, les termes de l'article 10 lui-même limitent le droit d'accès aux "données à caractère personnel concernant la personne concernée".

C. Les modalités de la réponse du responsable du traitement à la demande de la personne concernée

La principale exigence quant aux modalités de la réponse du responsable du traitement, tient au délai dans lequel il doit donner suite à la demande de la personne concernée. La loi prévoie en effet que "les renseignements sont communiqués sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande" (art. 10, § 1^{e}, al. 2). Cela signifie que le responsable est tenu de répondre le plus vite possible, le délai de 45 jours indiquant la durée maximum d'attente. Une dérogation est toutefois admise à l'article 10, § 3, lorsque la demande est introduite avant "l'expiration d'un délai raisonnable, à compter de la date d'une demande antérieure d'une même personne à laquelle il a été répondu ou de la date à laquelle les données lui ont été communiquées d'office". Que convient-il d'entendre par les termes "délai raisonnable"? Selon la doctrine, il convient de se référer à l'ancienne version de l'article, qui portant la limite à 12 mois. Les auteurs estiment donc que le délai raisonnable standard est d'une durée de 12 mois, ce délai pouvant être raccourci dans des cas exceptionnels ou quand les données ont été entre temps modifiées, à condition qu'il garde un caractère raisonnable. Ainsi, la doctrine considère qu'il ne doit être donné suite à une nouvelle demande que si les données ont substantiellement changé par rapport à la demande précédente[157].

Pour le reste, les seules indications légales relatives aux modalités de réponse résident dans son caractère compréhensible, ce qui laisse en principe le choix au responsable du traitement de procéder oralement ou par écrit, ainsi que la possibilité de moduler l'information à communiquer[158].

D. Les exceptions et le droit d'accès indirect

L'article 10 ne s'applique pas à tous les traitements, certains en demeurant exclus en raison de l'application modulée de la loi. Ils 'agit non seulement des traitements effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, dans la mesure où l'application de l'article 10 compromettrait une publication en projet ou fournirait des indications sur les sources d'information (art. 3, § 3 c)); et des traitements

[157] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 231-232.
[158] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 232-233.

effectués par la Sûreté de l'Etat, les autorités de police et le Centre européen pour enfants disparus et sexuellement exploités (art. 3, § 4, § 5 et § 6). Dans ces cas, l'article 13 de la loi offre à la personne concernée la possibilité d'exercer son droit d'accès de manière indirecte, c'est-à-dire via l'intermédiaire de la Commission de la protection de la vie privée. Celle-ci procède elle-même aux vérifications requises, et garantit donc à la personne concernée qui s'est adressée à elle qu'un contrôle du traitement de ses données à caractère personnel est assuré. L'arrêté royal d'exécution détermine en son chapitre V (art. 36 à 46) la procédure à suivre, les différentes conditions auxquelles est soumis le droit d'accès indirect, ainsi que le rôle de la Commission.

§ 4. – Le droit d'opposition

L'article 12 confère à la personne un droit d'opposition au traitement de ses données à caractère personnel, dans certains cas et moyennant le respect de certaines conditions, l'exercice de ce droit étant plus libre en cas de marketing direct.

A. Le droit général d'opposition

Ce que l'on entend par "droit général d'opposition" vise le droit d'opposition en dehors de l'hypothèse du marketing direct. C'est à l'article 12, § 1er, al. 2 qu'il est établi, en ces termes: "toute personne a en outre le droit de s'opposer, pour des raisons sérieuses et légitimes tenant à une situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf lorsque la licéité du traitement est basée sur les motifs visés à l'article 5, b) et c)". Ainsi, pareil droit d'opposition n'existe que lorsque le traitement est autorisé sur base de l'article 5, a), d), e), et f). Les deux cas qui demeurent exclus de cette disposition sont d'une part les traitements nécessaires à l'exécution d'un contrat auquel la personne concernée est partie, et d'autre part les traitements nécessaires au respect d'une obligation légale dans le chef du responsable du traitement. De plus, la demande d'opposition au traitement doit émaner de la personne concernée elle-même, celle-ci devant prouver son identité et se conformer à un certain nombre d'exigences légales – telles que le caractère écrit, daté et signé de la demande, par exemple. Enfin, la demande doit être motivée, l'opposition au traitement n'étant admise que "pour des raisons sérieuses et légitimes tenant à une situation particulière". Le qualificatif "sérieux" implique que la personne concernée prouve que le traitement entraine des effets désavantageux pour elle, tandis que l'adjectif "légitime" se réfère au caractère illégal du traitement, c'est-à-dire à l'absence de base légale l'autorisant[159].

Notons que l'opposition ne porte ici que sur les données, et non sur le traitement des données à caractère personnel de la personne concernée. "Ainsi, si les résultats scolaires d'un étudiant peuvent légitimement être communiqués par l'école secondaire à l'université, cet étudiant peut s'opposer non à la communication en tant que telle, mais à la communication d'une donnée particulière: doublement d'une année dû à des

[159] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 214.

circonstances familiales difficiles dans la mesure où cette information pourrait lui être préjudiciable"[160].

B. Le droit d'opposition en matière de marketing direct

Le troisième alinéa du paragraphe 1er de l'article 12 prévoit un droit d'opposition spécifique aux traitements de données à des fins de marketing, l'entourant de conditions moins strictes que le droit général d'opposition. En effet, même si les conditions relatives à l'identité de la personne concernée et aux formalités de la demande (signée et datée), la disposition prévoit que ce droit s'exerce gratuitement et sans justification. Il convient toutefois de bien circonscrire ce que recouvre la notion de "marketing direct", afin de déterminer l'ampleur de ce régime moins strict du droit d'opposition. Selon la Commission de la protection de la vie privée, il convient d'entendre par "marketing direct (vente en direct) toute offre de biens ou de services, à l'initiative de l'offrant, destinée à une personne spécifique"[161]. Un traitement aux fins de marketing direct vise donc toutes les opérations qui ont cela pour but, à savoir par exemple: la collecte et la vente de données à caractère personnel, les enquêtes de marché, la segmentation, la mise en place de profils, le fait d'opérer des sélections, etc.[162]. La recommandation R (85) 20 du 25 octobre 1985 du Comité des Ministres du Conseil de l'Europe, relative à la protection des données à caractère personnel utilisées à des fins de marketing direct offre une définition semblable: il convient d'entendre par marketing direct "l'ensemble des activités ainsi que tout service auxiliaire à celles-ci permettant d'offrir des produits et des services ou de transmettre tous autres messages publicitaires à des segments de population par le moyen du courrier, du téléphone ou d'autres moyens directs dans le but d'information ou afin de solliciter une réaction de la part de la personne concernée"[163]. Il résulte de ces définitions que le marketing direct doit davantage être considéré comme une technique, dans laquelle l'entretien et la perpétuation de la relation directe entre la personne concernée et celle qui l'approche est centrale, la nature de la finalité pour laquelle cette relation est créée ou entretenue étant moins pertinente, qu'elle soit commerciale, caritative, politique ou autre[164].

Dans quels cas le droit d'opposition en cas de marketing direct peut-il être exercé? L'article 12, § 1er, al. 3, vise différentes hypothèses, lesquelles sont au nombre de trois. Il importe de préciser que le marketing direct englobe tant les situations dans lesquelles le responsable du traitement traite lui-même les données, que les cas dans lesquels il les communique à un tiers qui les utilisera aux fins de marketing direct. La personne concernée peut tout d'abord s'opposer au traitement lorsque les données la concernant ont

---

[160] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 390.

[161] Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, http://www.privacycommission.be, p. 19.

[162] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 216.

[163] Recommandation n° R (85) 20 du 25 octobre 1985 du Comité des Ministres du Conseil de l'Europe aux Etats membres relative à la protection des données à caractère personnel utilisées à des fins de marketing direct, http://www.coe.int.

[164] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 216.

été collectées, auprès d'elle ou d'une tierce personne, à des fins de marketing direct. L'obligation d'information impose de porter à la connaissance de la personne concernée l'existence de son droit d'opposition au traitement. La seconde hypothèse est celle d'un responsable du traitement qui a collecté des données auprès de la personne concernée, et qui souhaite par après les traiter aux fins de marketing direct. Là encore, il devra informer la personne concernée de l'existence de son droit d'opposition. Est enfin visée la situation dans laquelle des données relatives à la personne concernée ont été récoltées autrement que directement auprès d'elle, et ont été communiquées, sans enregistrement, à un tiers. Cette dernière hypothèse vise par exemple le cas de la collecte de données via internet et leur transmission immédiate à un tiers[165].

L'arrêté royal d'exécution traite, en ses articles 34 et 35, des modalités d'information sur le droit d'opposition en matière de marketing direct. Trois situations sont prévues, la première visant celle où les données à caractère personnel sont collectées par écrit auprès de la personne concernée – via un formulaire ou coupon-réponse à remplir, par exemple. Dans ce cas, la possibilité doit être offerte à la personne concernée d'exercer son droit d'opposition sur le document par lequel elle communique ses données, via une case à cocher, par exemple (art. 34, al. 1er AR). Dans une seconde situation, les données sont récoltées auprès de la personne concernée autrement que par écrit – par téléphone ou caret à puce, par exemple –, auquel cas le responsable du traitement doit prendre contact avec elle pour lui demander si elle souhaite exercer son droit d'opposition. Il peut le faire soit sur un document qu'il lui communique à cette fin au plus tard deux mois après la collecte des données, soit par tout autre moyen technique permettant de garder la preuve de la possibilité qu'a eu la personne concernée d'exercer son droit d'opposition (art. 34, al. 2 AR). Enfin, l'article 35 prévoit une troisième situation, concernant les hypothèses dans lesquelles les données ne sont pas obtenues auprès de la personne concernée. Le responsable du traitement est alors tenu de lui demander par écrit si elle souhaite exercer son droit d'opposition, pareil exercice devant pouvoir se faire sur le document que le responsable du traitement lui adresse pour lui communiquer les informations prévues à l'article 9, § 2.

Contrairement au droit d'opposition général, il s'agit ici d'une opposition au traitement de ses données, et non aux seules données[166]. Notons que l'arrêté royal ne prévoit pas expressément la possibilité de moduler ce droit d'opposition, c'est-à-dire de ne s'opposer que partiellement à ce que certaines données soient traitées aux fins de marketing direct, sans que la personne concernée ne veuille s'opposer "en bloc" à ce que toutes ses données soient traitées à de telles fins. Il semble que dans ce cas rien n'oblige le responsable du traitement à communiquer ce refus partiel aux tiers auxquels il communiquerait les données[167].

---

[165] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 217.

[166] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 390.

[167] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 462.

C. Les conséquences de l'exercice du droit d'opposition

L'alinéa 4 de l'article 12, § 1er énonce « qu'en cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données ». Le droit d'opposition n'a donc pas un caractère général, la personne concernée ne pouvant s'opposer au traitement en tant que tel, mais uniquement au traitement de ses données à caractère personnel, en tout ou en partie[168].

§ 5. – Le droit de rectification

La personne concernée a en outre le droit d'obtenir sans frais la rectification de données inexactes la concernant. Si l'article 12, § 1er, al. 1er emploie les termes de "toute personne", l'article 12, § 2 précise que seule la personne concernée elle-même – ou son représentant légal – peut exiger la rectification de ses données à caractère personnel. La demande doit être datée et signée, mais la loi n'exige pas que la personne concernée apporte la preuve de son identité. Cela est toutefois nécessaire en pratique, ne fut-ce que pour le contrôle, par le responsable du traitement, de la validité juridique de la demande[169].

Le concept de rectification ne se réfère pas uniquement aux corrections purement matérielles. Au contraire, il englobe la correction de données inexactes relatives à la personne concernée (art. 12, § 1er, al. 1er); la "suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel la concernant qui, compte tenu du but du traitement, est incomplète ou non pertinente ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée" (art. 12, § 1er, al. 5); et enfin le complément de données la concernant. L'ampleur de ce droit est donc relativement large, ne conférant toutefois pas le droit à la personne concernée de rectifier des appréciations ou jugements subjectifs[170].

Le responsable du traitement est tenu de donner suite à la demande dans le mois qui suit l'introduction de la requête. Il informe la personne concernée des rectifications qu'il a opérées, ainsi que des personnes à qui il les a communiquées. Cette dernière obligation ne lui est imposée que s'il a encore "connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés" (art. 12, § 3). Aucune précision légale n'impose une forme particulière pour la réaction du responsable du traitement, un écrit étant toutefois recommandé afin d'être en mesure de prouver qu'il a dûment répondu à la demande de la personne concernée.

Notons que l'article 15, qui traite de l'action en justice qui peut être introduite par la personne concernée – et que nous examinerons ci-dessous –, précise que le responsable du traitement doit indiquer que telle donnée est contestée à chaque communication de celle-ci, tant qu'aucune décision ayant force de chose jugée n'intervient. Précisons enfin que le droit de rectification peut s'exercer indirectement, via l'intermédiaire de la

[168] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 218-219.
[169] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 237.
[170] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 219-220.

Commission de la protection de la vie privée, conformément à l'article 13 de la loi, dont nous avons examiné le contenu ci-dessus.

§ 6. – Le droit de ne pas être soumis à des décisions individuelles automatiques

Avec les progrès sans cesse croissants de l'informatique, qui caractérisent notre société actuelle, de plus en plus de décisions concernant les citoyens sont prises sur base de traitements automatisés. Le risque est grand de rendre ces décisions totalement dépourvues de toute intervention humaine, étant la seule conséquence d'une procédure informatique[171]. C'est pourquoi l'article 12 *bis* de la loi relative à la protection de la vie privée, introduit lors de la transposition de la directive européenne en 1998, interdit qu'une "décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne [puisse] être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité".

Plusieurs conditions doivent être satisfaites pour l'application de cette interdiction, la première exigeant que des effets juridiques soient attachés à la décision, ou que celle-ci affecte la personne concernée de manière significative. En outre, la décision ne doit être prise que sur base d'un traitement automatisé: si une intervention humaine, même minime, participe à la décision, l'interdiction de l'article 12 *bis* ne s'applique pas. Enfin, la prohibition ne vise que les traitements de données à caractère personnel visant à évaluer certains aspects de la personnalité de la personne concernée. Demeure par exemple ainsi exclu de l'application de cette disposition, le traitement qui autorise ou refuse un retrait d'argent à un guichet automatique sur base du solde du compte, pareil traitement n'ayant pour but de juger aucun aspect de la personnalité[172].

Le législateur a toutefois prévu deux exceptions à cette interdiction de principe, à savoir les décisions prises dans le cadre d'un contrat ou fondées sur une disposition légale. Ces exceptions sont toutefois assorties de garanties, la loi exigeant que l'instrument contractuel ou légal prévoyant cette décision contienne "des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé". En particulier, "il devra au moins être permis à celui-ci de faire valoir utilement son point de vue" (art. 12 *bis* al. 2).

A titre de garantie supplémentaire, rappelons que l'article 10, § 1er, c) prévoit que la personne concernée a le droit d'obtenir du responsable du traitement "la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas des décisions automatisées visées à l'article 12bis".

§ 7. – Le droit d'introduire un recours en justice

Nous n'entrerons pas dans les détails judiciaires et procéduraux qu'offrent la loi du 8 décembre 1992 relative à la protection de la vie privée, ceux-ci n'étant que très peu

[171] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 219.
[172] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 220.

pertinents en matière de santé publique. Notons simplement que la personne concernée a la possibilité de s'adresser à plusieurs instances, afin de pouvoir contraindre le responsable du traitement au respect de ses droits. Ainsi, outre le droit d'exercer indirectement ses droits via l'intermédiaire de la Commission de la protection de la vie privée (art. 13), la personne concernée peut introduire une plainte auprès de celle-ci (art. 31), tout comme elle peut s'adresser au président du tribunal de première instance pour qu'il tranche un litige relatif à l'exercice de ses droits (art. 14 et 15). Enfin, elle est en mesure d'obtenir réparation du dommage que le non respect de la loi par le responsable du traitement lui cause (art. 15 *bis*), et ce selon un système de responsabilité sans faute, autrement dit de responsabilité objective[173].

Section III. – Les mécanismes de contrôle

Il ne suffit pas d'établir des règles et de reconnaitre des droits en faveur de la personne concernée pour garantir la protection de la vie privée de celle-ci, encore faut-il être en mesure que la loi est bel et bien appliquée et respectée. C'est la raison pour laquelle divers mécanismes de contrôle sont instaurés, qu'il s'agisse de contrôle interne – traduit dans un certain nombre d'obligations à charge du responsable du traitement en matière de sécurité et de confidentialité du traitement –, ou externe – à savoir les obligations qui lui incombent envers la Commission de la protection de la vie privée.

§ 1er. – Le contrôle interne: les obligations en matière de sécurité et de confidentialité du traitement

L'article 16 de la loi du 8 décembre 1992 énonce un certain nombre d'obligations qui incombent au responsable du traitement, lesquelles constituent les mesures de contrôle interne, à savoir celles relatives à la sécurité et à la confidentialité du traitement. Il s'agit donc d'obligations d'ordre technique et organisationnel, contrairement à l'obligation prévue par l'article 17 et relative à la déclaration auprès de la Commission de la protection de la vie privée, qui est d'ordre administratif et dont nous traiterons lors de l'examen des mécanismes de contrôle externe, au cours du paragraphe suivant.

Le contrôle interne consiste en quatre obligations à charge du responsable du traitement, obligations que nous examinerons non pas en suivant l'ordre de la disposition légale, mais selon leur degré d'importance.

A. Obligations en matière de sécurité des données à caractère personnel

Bien que la loi énonce cette obligation en dernier lieu, il semble qu'elle soit essentielle au respect d'un chapitre intitulé "De la confidentialité et de la sécurité du traitement". Le responsable du traitement est donc tenu, "afin de garantir la sécurité des

[173] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 243. Pour plus de détails à ce sujet, voyez les pages 240-246.

données à caractère personnel", de prendre "toutes 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" (art. 16, § 4, al. 1er). Notons que la loi belge, en empruntant les termes de "traitement non autorisé", se montre moins large que la directive européenne, qui emploie les termes de "traitement illicite"[174].

Le second alinéa de la disposition précise le **niveau de protection adéquat** qui doit être garanti, et niveau tenant compte "d'une part, de l'état de la technique en la matière et des frais qu'entraine l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels". La loi prévoit donc quatre critères pour déterminer quel niveau de protection est adéquat au traitement en question. Si l'appréciation du caractère adéquat du niveau de protection revient dans un premier temps au responsable du traitement, la Commission et les tribunaux n'en sont pas moins compétents pour exercer une certaine tutelle à ce sujet[175]. Un premier critère à prendre en considération est relatif à la nature des données traitées, ce qui se réfère non seulement à la distinction entre les catégories particulières de données (sensibles, relatives à la santé et judiciaires) et les autres, les premières nécessitant plus de protection que les secondes; mais aussi à l'intérêt sociétal et/ou économique que portent les données. Ainsi convient-il d'accorder une plus grande protection aux données financières, par exemple[176]. La nature des risques potentiels entre également en ligne de compte, ceux-ci étant principalement déterminés par la nature des données traitées, ainsi que par le nombre de personnes qui y auront accès. Le troisième critère se réfère à l'état de la technique, ce qui pourrait paraitre clément à l'égard du responsable du traitement, celui-ci n'étant pas tenu à un niveau de protection supérieur à ce que l'avancement des techniques permet. Cependant, ce critère met à sa charge une obligation d'information permanente: il doit sans cesse se mettre au courant des nouvelles techniques, s'informer et rechercher de manière active ce qu'il est possible de faire. L'on considère que le responsable du traitement pourra se limiter aux techniques qui sont commercialisées, et qui lui sont effectivement disponibles[177]. Enfin, le dernier critère concerne les coûts de l'application des mesures de sécurité, ce qui signifie que le responsable du traitement ne peut être excessivement économe. Les coûts ne doivent pas nécessairement être illimités, mais ils doivent rester raisonnables au regard non seulement des moyens financiers du responsable du traitement, mais également de l'avantage qu'il retirera de ce traitement. Il résulte de cette analyse que le responsable du traitement est soumis non pas à une obligation de résultat, mais bien à une obligation de moyens. Il est tenu de tout mettre en œuvre pour garantir un niveau de protection adéquat, mais ne pourra être sanctionné que s'il n'est pas en mesure de prouver que le manque de protection de son traitement existe malgré le respect des critères énoncés par

---

[174] Directive européenne 95/46/C.E. 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.,* L 281/31, 23 nov. 1995, http://www.eur-lex.europa.eu (art. 17.1, al. 1er). Pour plus de détails à ce sujet, voyez D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 249.

[175] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 252-253.

[176] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 253.

[177] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 253.

la loi. Il est donc tenu de prendre les mesures que prendrait un responsable de traitement normalement diligent et prudent[178].

Concrètement, en qui consistent ces fameuses mesures à prendre? A part l'énonciation des critères relatifs au niveau de protection à garantir, la loi est muette à ce sujet. C'est donc vers la doctrine et vers d'autres instruments qu'il nous faut nous tourner, comme par exemple la Recommandation R (97) 5 du Conseil de l'Europe concernant la protection des données médicales[179], qui propose, en son article 9.2 une petite dizaine de mesures visant à la confidentialité, l'intégrité et l'exactitude des données traitées, ainsi qu'à la protection des patients. Il nous semble utile de reproduire la disposition ici, afin de se faire une idée de ce que représentent ces mesures de sécurité:

9.2. *Afin notamment d'assurer la confidentialité, l'intégrité et l'exactitude des données traitées, ainsi que la protection des patients, des mesures appropriées devraient être prises visant:*
a. *à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations);*
b. *à empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports de données);*
c. *à empêcher l'introduction non autorisée de données dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées (contrôle de mémoire);*
d. *à empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);*
e. *en vue, d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, à assurer que leur traitement soit en règle générale conçu de façon à permettre la séparation:*
- des identifiants et des données relatives à l'identité des personnes;
- des données administratives;
- des données médicales;
- des données sociales;
- des données génétiques (contrôle d'accès);
f. *à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication);*
g. *à garantir qu'il puisse être vérifié et constaté a posteriori qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction);*
h. *à empêcher que, lors de la communication de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);*
i. *à sauvegarder les données par la constitution de copies de sécurité (contrôle de disponibilité).*

S'avère également éclairante à ce sujet la Recommandation du Conseil de l'OCDE, du 29 novembre 1992, concernant les "guidelines for the security of information systems"[180].

Sur base de ces divers instruments et de la doctrine, il semble que les mesures de sécurité puissent se regrouper en deux catégories, la première concernant les **mesures de sécurité techniques**. Elles peuvent se diviser à leur tour en mesures physiques et en

[178] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 254.
[179] Recommandation n° R(97) 5 du 13 février1997 du Comité des Ministres du Conseil de l'Europe aux Etats membres relative à la protection des données médicales, http://www.coe.int.
[180] OECD Guidelines for the Security of Information Systems, 26 novembre 1992, http://www.oecd.org/document/19/0,3343,fr_2649_201185_1815059_1_1_1_1,00.html.

mesures logiques. Les premières visent à protéger le système lui-même, contre une destruction générale, pour cause d'incendie par exemple. Il s'agit de placer les ordinateurs dans un local sécurisé, de limiter l'accès à certains espaces en le soumettant à un système d'identification par badges ou à une application biométrique. De la même manière, les fichiers, disquettes et autres supports doivent être conservés en lieux sécurisés, dont l'accès de tierces personnes est surveillé. Quant aux mesures logiques, elles sont destinées à protéger les applications software, entre autres contre le hacking et la piraterie informatique. Il s'agit donc de mesures de codage et de cryptage des données, auquel peut s'ajouter l'emploi de mots de passe. Notons que ces mesures de sécurité techniques ne doivent pas seulement être mises en œuvre lors de l'exécution du traitement, mais également dès sa conception[181].

La seconde catégorie vise les **mesures de sécurité organisationnelles**, lesquelles ont trait aux aspects qui ne peuvent être réglés sur le plan technique, comme par exemple l'avertissement et l'information des membres du personnel. Il s'agit donc, entre autres, d'établir certaines "polices", consistant par exemple en "clean desk policy", en l'interdiction de ramener des données à caractère personnel à son domicile, ou encore au bon usage des mots de passe. L'on y inclut également l'introduction d'un devoir de confidentialité (secret professionnel) contractuel.

B. Les obligations techniques et organisationnelles concrètes

L'article 16, § 2, met à charge du responsable du traitement quatre obligations concrètes, concernant la sécurité et la confidentialité des données, auxquelles il devra se conformer en plus de prendre les mesures de sécurité visant à assurer un niveau de protection adéquat. Il s'agit tout d'abord de devoir "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" (art. 16, § 2, 1°). Cette obligation peut se résumer en un devoir de souci de qualité.

Le responsable du traitement doit en outre limiter l'accès aux données, et ce de deux manières. Non seulement, ne peuvent y avoir accès que les personnes qui en ont besoin pour l'exercice de leurs tâches ou pour les besoins de leur service, mais en outre cet accès est limité aux données dont elles ont besoin. Dans les deux cas, le critère est "need to know", et non "nice to know"[182].

Une troisième obligation réside dans l'information que le responsable du traitement doit fournir aux personnes agissant sous son autorité, à propos de la loi relative à la protection de la vie privée, de ses arrêtés d'exécution et de toute autre mesure pertinente à ce sujet. En bref, il doit porter à leur connaissance l'existence et le contenu toute réglementation relative à la vie privée qui leur est applicable. Le critère selon lequel il convient de déterminer quelle information est pertinente est celui du but du traitement dont il s'agit. En effet, les réglementations pertinentes ne seront pas les mêmes en cas de traitement par une institution financière, et de traitement en matière de relations de travail. La loi ne précisant pas la manière dont l'information doit être fournie, le

[181] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 250-251.
[182] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 256.

responsable du traitement est libre de choisir comment il informera les personnes agissant sous son autorité, que ce soit par écrit ou par moyens électroniques[183].

Enfin, le responsable du traitement est tenu de s'assurer de la "conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration de l'article 17 ainsi que de la régularité de leur application" (art. 16, § 2, 4°). Les auteurs considèrent que ce devoir de conformité s'applique même si le responsable du traitement se trouve dans un cas de dispense à l'obligation de déclaration auprès de la Commission de la protection de la vie privée. De plus, la doctrine estime que ce devoir ne concerne pas seulement les traitements automatisés, le responsable de tout traitement étant tenu de vérifier qu'il est en conformité avec la déclaration, également en ce qui concerne la finalité du traitement[184].

C. Relation avec le sous-traitant

La première obligation que l'article 16 impose au responsable du traitement concerne la relation qu'il entretient avec le sous-traitant auquel il confie le traitement. Un premier aspect de cette obligation limite le choix du sous-traitant par le responsable du traitement, celui-ci étant tenu de "choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements" (art. 16, § 1er, 1°). Il doit donc d'initiative demander au sous-traitant une description des mesures qu'il applique, et ce de préférence par écrit, afin de pouvoir s'assurer la preuve que le sous-traitant offrait des garanties suffisantes. Cela peut par exemple faire partie des conditions de l'offre[185].

Le responsable du traitement doit en outre veiller au respect de ces mesures, "notamment par la stipulation de mentions contractuelles" (art. 16, § 1er, 2°), ce qui ne l'empêche pas d'y veiller par d'autres moyens, comme par exemple un contrôle d'audit. La réalisation de cette obligation dépendra des circonstances du cas d'espèce.

La responsabilité du sous-traitant doit être fixée dans le contrat de sous-traitance. Cela permettra par exemple au responsable du traitement d'échapper à sa responsabilité objective établie à l'article 15 *bis*, pareille disposition lui permettant de prouver que le fait qui a causé le dommage à la personne concernée relève de la responsabilité du sous-traitant. Une fois de plus, il conviendra de tenir compte des circonstances de l'espèce dans cette appréciation.

Le contrat de sous-traitance doit également préciser que le sous-traitant n'agit que sur les instructions du responsable du traitement, et est soumis aux mêmes obligations que lui.

En résumé, le contrat de sous-traitance devra contenir les éléments suivants:

- Les mesures de sécurité techniques et organisationnelles relatives au traitement en cause;
- La responsabilité du sous-traitant;
- Le principe selon lequel le sous-traitant agit pour le compte du responsable du traitement;

[183] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 258-259.
[184] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 259.
[185] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 260-261.

- Le principe selon lequel le sous-traitant est soumis aux mêmes obligations que le responsable du traitement.

L'article 16, § 1er, 5° précise que ces éléments du contrat doivent être consignés par écrit ou sur un support électronique[186].

D. La confidentialité du traitement

Une dernière obligation à charge du responsable du traitement vise à prendre en compte le fait que les risques liés au traitement de données à caractère personnel ne proviennent pas uniquement d'actes externes posés par des tiers. En effet, l'usage non autorisé de pareilles données, par des personnes agissant sous l'autorité du responsable du traitement, peut également porter atteinte à la vie privée de la personne concernée. C'est pourquoi l'article 16, § 3 prévoit que les personnes agissant sous l'autorité du responsable du traitement ne peuvent traiter les données que sur instruction de celui-ci. Cette disposition contient donc deux obligations distinctes, selon la personne qui y est tenue: le responsable du traitement doit donner des instructions, tandis que les personnes agissant sous son autorité doivent les respecter. Ainsi, un traitement de données à caractère personnel effectué par une personne agissant sous l'autorité du responsable du traitement, qui n'est pas en conformité avec les instructions de celui-ci, est considéré comme illicite[187]. Une seule exception n'est prévue, à savoir le cas d'une obligation légalement imposée.

§ 2. – Le contrôle externe: la déclaration auprès de la Commission de la protection de la vie privée et les compétences de celle-ci

Le contrôle externe est de deux types: *a priori* et *a posteriori.* Dans la première catégorie se trouvent la déclaration de traitement que tout responsable de traitement doit remettre à la Commission de la protection de la vie privée, ainsi que l'avis préalable de celle-ci et les éventuelles recommandations qui l'accompagnent. Au rang du contrôle externe *a posteriori* se situent les divers recours administratifs et juridictionnels qui peuvent être exercés une fois le traitement mis en place. Ainsi que nous l'avons déjà évoqué ci-dessus, nous n'entrerons pas dans les détails judiciaires et procéduraux des recours juridictionnels. De plus, si la directive européenne offre aux Etats membres la possibilité de prévoir des recours administratifs – le recours juridictionnel étant imposé –, le législateur belge n'a pas saisi cette opportunité de conférer à la Commission de la protection de la vie privée (CPVP) la qualité de chambre de recours dont la saisie serait préalable à un recours juridictionnel[188]. C'est donc principalement les mécanismes de contrôle *a priori* qui feront l'objet de notre attention ici.

---

[186] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 262-263.
[187] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 263-264.
[188] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, pp. 393-394.

L'instrument de contrôle principal dont dispose la CPVP est la déclaration de traitement que doit remettre lui tout responsable de traitement automatisé. S'ajoute à cette formalité celle de l'inscription au registre public tenu par la CPVP. La déclaration et l'inscription au registre répondent à une double préoccupation, à savoir l'information du public – afin de lui permettre de trouver les éléments nécessaires à l'exercice de ses droits, ainsi que d'avoir une vue d'ensemble des utilisations de données personnelles en Belgique – et l'information de la Commission – afin de lui permettre d'exercer ses missions de contrôle et de traitement des plaintes. Certaines informations restent toutefois confidentielles[189].

La loi prévoit en outre les règles de composition et de fonctionnement de la CPVP, parmi lesquelles figure la possibilité de créer des Comités sectoriels.

A. La déclaration

1) De quels traitements s'agit-il?

L'article 17, § 1er impose au responsable du traitement de remettre à la CPVP, préalablement à la mise en œuvre d'un **traitement entièrement ou partiellement automatisé** de données à caractère personnel, une déclaration de ce traitement. Seuls les traitements automatisés sont soumis à cette formalité, pour des raisons liées aux risques qu'ils présentent, ainsi qu'à l'efficacité du contrôle de la Commission, efficacité qui requiert que cette dernière se concentre sur ce type de traitements[190]. Toutefois, l'article 19 permet à la CPVP d'exiger la remise de pareille déclaration pour un **traitement non automatisé** de données à caractère personnel contenues ou appelées à figurer dans un fichier, lorsqu'elle estime que ce traitement est susceptible de porter atteinte à la vie privée. Elle peut exercer cette compétence soit d'initiative, soit sur requête d'une personne concernée.

L'article 17, § 5 apporte une certaine confusion, voire une contradiction[191], en énonçant que "chaque finalité ou ensemble de finalités liées pour lesquelles il est procédé à un ou à plusieurs traitements partiellement ou totalement automatisés doit faire l'objet d'une déclaration". En effet, non seulement l'article 17, § 1er parle de déclaration de traitement et non de finalité, mais en plus le § 3 mentionne la finalité du traitement parmi les informations que doit contenir la déclaration. L'exposé des motifs conclut que l'objet de la déclaration n'est en fait pas le traitement en tant que tel, mais bien "les finalités éventuellement liées par lesquelles un ou plusieurs traitements sont effectués"[192]. Un traitement poursuivant diverses finalités devrait donc faire l'objet de plusieurs

[189] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Commentaire des articles, *Doc. Parl.,* Ch. repr., sess. ord.1990-1991, n° 47K1610001 du 6 mai 1991, p. 22, http://www.lachambre.be.

[190] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Commentaire des articles, *Doc. Parl.,* Ch. repr., sess. ord.1990-1991, n° 47K1610001 du 6 mai 1991, p. 21, http://www.lachambre.be.

[191] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 392.

[192] Exposé des motifs, p. 55.

déclarations si les finalités ne sont pas liées. Comment évaluer cette liaison? La question fait l'objet de nombreux débats doctrinaux, dans les détails desquels nous n'entrerons pas ici. Il semble que la contradiction doive être tranchée à la lumière du but de transparence que la déclaration doit remplir. Il s'agit en fait d'éviter que certains traitements ne soient pas déclarés: en effet, si les finalités d'un même traitement sont "incompatibles ou non liées, il s'agit en fait de plusieurs traitements qui doivent donner lieu à différentes déclarations"[193]. Quant à la question de savoir si les finalités d'un ou plusieurs traitements sont liées ou non, cela dépend des circonstances de fait. Un lien clair doit exister entre les finalités de plusieurs traitements, de telle sorte que le défaut de remettre des déclarations distinctes ne crée aucun risque d'atteinte à la vie privée de la personne concernée[194].

Une **exception** est prévue par la loi, la déclaration n'étant pas requise en cas de traitement automatisé lorsque celui-ci a pour seul objet la tenue d'un registre destiné à l'information du public et ouvert à celui-ci, en vertu d'une loi, d'un décret ou d'une ordonnance (art. 17, § 1e, al. 2). Il s'agit par exemple du registre du commerce. Cette exception se justifie par le fait que tant la CPVP que le public sont déjà au courant de l'existence de ce registre pour la tenue duquel des données à caractère personnel sont traitées. La loi précise cependant qu'il doit s'agir du seul objet du traitement, la réalisation d'une autre finalité à l'aide de ce traitement entrainant l'obligation de le déclarer à la CPVP[195].

D'autres **exceptions** peuvent être prévues par arrêté royal, "lorsque, compte tenu des données traitées, il n'y a manifestement pas de risque d'atteinte aux droits et libertés des personnes concernées et que sont précisées [dans l'arrêté royal] les finalités du traitement, les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données" (art. 17, § 8, al. 1er). Les informations à mentionner dans la déclaration devront toutefois être communiquées par le responsable du traitement à toute personne qui en fait la demande (al. 2). En outre, il ne s'agit pas d'exceptions totales mais partielles, seuls les §§ 3 à 6 étant visés. Les autres dispositions de l'article 17 sont à respecter, la Commission demeurant par exemple en mesure d'exiger que certaines informations lui soient fournies (art. 17, § 4). Enfin, ces exceptions ne peuvent être invoquées que si les conditions sont respectées, ces conditions étant prévues par l'arrêté royal et tenant aux finalités du traitement, aux catégories de données traitées, aux catégories de personnes concernées, aux catégories de destinataires et à la durée de conservation des données. L'arrêté royal d'exécution décrit, en ses articles 51 à 62, un certain nombre de catégories de traitements exemptées de l'obligation d'information. Nous n'entrerons pas dans les détails de chacune des situations prévues, nous contentant de les citer et de mentionner l'une ou l'autre précision pertinente en matière de santé publique. Sont donc exemptés de l'obligation d'information:

- Les traitements nécessaires à l'administration des salaires des personnes au service du ou travaillant pour le responsable du traitement (art. 51);

[193] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 393.
[194] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 269.
[195] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 266.

- Les traitements qui visent l'administration du personnel au service du ou travaillant pour le responsable du traitement (art. 52);
- Les traitements qui se rapportent à la comptabilité du responsable du traitement (art. 53);
- Les traitements qui visent l'administration d'actionnaires ou d'associés (art. 54);
- Les traitements qui visent la gestion de la clientèle ou des fournisseurs (art. 55);
- Les traitements effectués dans une fondation, une association ou tout autre organisme sans but lucratif dans le cadre de leurs activités ordinaires (art. 56);
- Les traitements indispensables à la communication effectués dans le seul but d'entrer en contact avec l'intéressé (art. 57);
- Les traitements portant sur l'enregistrement de visiteurs effectués dans le cadre d'un contrôle d'accès (art. 58);
- Les traitements par les établissements d'enseignement en vue de gérer leurs relations avec leurs élèves ou étudiants (art. 59);
- Les traitements effectués par les communes relatifs aux registres de la population et aux cartes d'identité, et les traitements effectués par des autorités administratives si le traitement est soumis à des réglementations particulières adoptées par ou en vertu de la loi et réglementant l'accès aux données traitées ainsi que leur utilisation et leur obtention (art. 60 et 61);
- Les traitements de données personnelles gérées par les institutions de sécurité sociale visées dans la loi du 15 janvier 1990 relative à l'institution d'une Banque-carrefour de la sécurité sociale, à condition qu'elles respectent les dispositions de cette loi (art. 62).

La dernière catégorie de traitement nous intéresse particulièrement ici. Cette exemption vise à éviter un double emploi avec le système de déclaration de la Banque-carrefour, laquelle oblige toute institution de sécurité sociale à déclarer les traitements à son Comité de surveillance, et met à disposition de la CPVP les informations qu'elle détient dans ce cadre[196].

2) Quand faut-il remettre une déclaration?

La déclaration ne doit pas uniquement être remise à la CPVP préalablement à la mise en œuvre d'un traitement automatisé. Cette obligation incombe également au responsable du traitement en cas de suppression d'un traitement automatisé, ainsi que lors de toute modification d'une des informations contenues dans la déclaration (art. 17, § 7). Selon la Commission, il convient d'entendre par "modification", toute modification de nom dans les rubriques qui concernent le responsable du traitement, et toute modification de changement d'une des rubriques relatives au traitement lui-même[197].

Un cas particulier est celui de la fusion ou de la reprise de fichiers. Si un fichier est repris par un responsable qui en possède déjà un semblable et dont les déclarations sont identiques, une nouvelle déclaration n'est pas nécessaire, la reprise devant seulement

[196] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 464.
[197] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 270.

être mentionnée à la CPVP. Si par contre, lors d'un transfert de fichier, les données ne sont pas identiques, il s'agit d'une modification, et donc une déclaration doit en être faite. Cela ne vaut qu'à condition que le responsable qui reprend le fichier le fasse sous le même nom. Si la dénomination du traitement change, ou si la finalité change, une nouvelle déclaration doit être faite[198].

3) Que doit contenir la déclaration?

L'on croit souvent que la formalité de la déclaration implique que toutes les données à caractère personnel qui sont traitées doivent être communiquées à la Commission. Rien n'est moins vrai, la déclaration se limitant à une description des caractéristiques générales du traitement. Le but de la manœuvre est d'assurer la publicité des finalités et des caractéristiques du traitement, afin de rendre la CPVP en mesure de vérifier que les dispositions de la loi sont respectées, et que la vie privée des personnes concernées est protégée. L'article 17, § 3 énumère un certain nombre d'éléments qui doivent figurer dans la déclaration, auxquels s'ajoutent des informations supplémentaires dans certains cas (art. 17, § 6, et arrêté royal d'exécution).

C'est ainsi que toute déclaration doit mentionner (art 17, § 3):

- la date de la déclaration et, le cas échéant, la mention de la loi, du décret, de l'ordonnance ou de l'acte réglementaire décidant la création du traitement automatisé;
- les nom, prénoms et adresse complète ou la dénomination et le siège du responsable du traitement et, le cas échéant, de son représentant en Belgique;
- la dénomination du traitement automatisé;
- la finalité ou l'ensemble des finalités liées du traitement automatisé;
- les catégories de données à caractère personnel qui sont traitées avec une description particulière des données visées aux articles 6 à 8;
- les catégories de destinataires à qui les données peuvent être fournies;
- les garanties dont doit être entourée la communication de données aux tiers;
- les moyens par lesquels les personnes qui font l'objet des données en seront informées, le service auprès duquel s'exercera le droit d'accès et les mesures prises pour faciliter l'exercice de ce droit;
- la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées.
- une description générale permettant d'apprécier de façon préliminaire le caractère approprié des mesures prises pour assurer la sécurité du traitement en application de l'article 16 de cette loi;
- les motifs sur lesquels le responsable du traitement fonde, le cas échéant, l'application de l'article 3, § 3, de la présente loi.

Rappelons que la Commission peut, sur base de l'article 17, § 4, exiger du responsable du traitement qu'il lui communique d'autres éléments d'information. En outre, des informations supplémentaires doivent être mentionnées lorsque les données sont destinées à être transmise vers l'étranger – c'est-à-dire vers un pays non membre de

[198] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 270.

l'Union européenne, les Etats membres de l'UE étant supposés garantir le même niveau de protection, en vertu de la directive européenne –, même si la transmission n'est qu'occasionnelle. Dans ce cas, devront être indiqués non seulement les catégories de données transmises, ainsi que le pays de destination. Le but est de pouvoir vérifier que le niveau de protection assuré par le pays de destination est suffisant. Enfin, l'arrêté royal d'exécution impose des mentions supplémentaires en cas de traitement ultérieur à des fins historiques, statistiques ou scientifiques (art. 4, 5, 16 et 21 AR), ainsi qu'en cas de traitement de catégories particulières de données (art. 25, 4° AR), et d'exemption à l'obligation d'information visée à l'article 9, § 2 de la loi (art. 31 AR).

4) Comment faut-il déclarer un traitement?

La loi ne précise pas la manière dont la déclaration doit être remise, laissant à la Commission le soin d'en déterminer la nature et la structure (art. 17, § 5, al. 2). C'est ainsi que l'usage des supports établis par la CPVP est obligatoire, celle-ci laissant toutefois le choix au responsable du traitement d'utiliser le formulaire de déclaration papier ou le formulaire électronique, via le support d'information magnétique mis à disposition par la CPVP[199].

5) Quelles sont les autres formalités à accomplir lors de la remise de la déclaration?

La loi prévoit, en son article 17, § 9, que le responsable du traitement est tenu de verser, lors de l'accomplissement de toute déclaration, une contribution destinée à couvrir les frais de fonctionnement de la Commission[200]. Le législateur laisse au Roi le soin de déterminer le montant de cette contribution, ainsi que les modalités de paiement, tout en fixant une limite que ce montant ne peut dépasser. L'arrêté royal exécute, en ses articles 47 à 50, adaptant le montant à payer en fonction entre autres du support utilisé – écrit ou électronique, ce dernier étant favorisé par un tarif réduit. En outre, un prix forfaitaire est prévu en cas de déclarations simultanées, le responsable ne payant qu' « un seul et même montant pour toutes les informations qu'il déclare à la Commission à la même occasion. Le nombre de finalités ou de finalités liées que le responsable distingue à cette occasion, de même que le nombre de formulaires sur lesquels sont répartis la déclaration importent peu »[201]. Quant au mode de paiement, il doit se faire au moyen des documents mis à disposition par la CPVP.

6) Quel rôle joue la CPVP?

Bien que la déclaration doive être remise préalablement à la mise en œuvre du traitement, le responsable n'est pas tenu d'attendre l'accord de la CPVP pour pouvoir

[199] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 275.
[200] Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Commentaire des articles, *Doc. Parl.,* Ch. repr., sess. ord.1990-1991, n° 47K1610001 du 6 mai 1991, p. 23, http://www.lachambre.be.
[201] C. DE TERWANGNE et S. LOUVEAUX, "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 463.

réaliser ce traitement. La CPVP n'est en effet pas tenue de réagir à la déclaration, ce qui signifie que l'absence de réaction ne peut être considérée comme garantie de la légalité du traitement. Le rôle de la Commission est donc grandement réduit, se limitant à la remise d'un accusé de réception – prouvant que la déclaration a été introduite, et jouant un plus grand rôle en cas de traitement ultérieur à des fins historiques, statistiques ou scientifiques, les données codées ne pouvant être transmises au responsable du traitement ultérieur que sur présentation de l'accusé de réception relatif à ce traitement ultérieur – ainsi qu'à la vérification du caractère complet de la déclaration.

L'obligation de déclaration ne poursuit donc qu'une fin de transparence et de publicité, n'étant pas soumise à un contrôle automatique, et ne devant être suivie d'aucun accord de principe. Cela dit, c'est au travers des informations qu'elle reçoit via les déclarations de traitement que la CPVP sera en mesure d'exercer ses compétences d'avis, de recommandations et de traitement des plaintes, ainsi que nous le verrons ci-dessous. En outre, si le contrôle effectué par la CPVP s'avère relativement faible, une disposition particulière a été adoptée pour les traitements dits à risque, afin de conformer la loi belge à la directive européenne. En effet, l'article 17 *bis* de la loi confère au Roi le pouvoir de déterminer "les catégories de traitements qui présentent des risques particuliers au regard des droits et libertés des personnes concernées", et de fixer "des conditions particulières pour garantir les droits et libertés des personnes concernées". Le Roi pourrait ainsi qualifier certains traitements comme étant à risque, et les soumettre à certaines garanties supplémentaires. Malheureusement, aucun arrêté royal n'a à ce jour été adopté à ce sujet, l'article 17 *bis* ne pouvant donc être appliqué actuellement.

B. Le registre public

L'ensemble des déclarations communiquées à la CPVP est destiné à figurer dans un registre public, tenu auprès de celle-ci. Le but de ce registre est double: il s'agit non seulement de permettre à la personne concernée de trouver toutes les informations nécessaires à l'exercice de ses droits, mais également de procurer une vue d'ensemble de tout ce qui est réalisé en Belgique avec les données à caractère personnel[202]. L'article 18 de la loi prévoit que "l'inscription au registre contient les indications visées à l'article 17, §§ 3 et 6". Les traitements exemptés de l'obligation d'information ne sont donc en principe pas inscrits au registre public, la CPVP pouvant toutefois exiger la communication des informations figurant dans la déclaration, et les inscrire au registre. En outre, s'il s'agit d'un traitement pour lequel des informations supplémentaires sont exigées, celles-ci figureront également dans le registre.

Trois voies d'accès au registre ont été prévues par l'arrêté royal (art. 63), cet accès étant en tous les cas gratuit et soumis à aucune obligation de justification des raisons de la consultation (art. 68 et 69 AR). La première forme d'accès consiste en une consultation directe à distance, par le biais de moyens de télécommunication (art. 63, a)), laquelle se réalise par la mise à disposition par la CPVP d'une copie du registre public sur un serveur accessible via internet (art. 64). Une seconde possibilité est la consultation directe sur place dans les locaux désignés à cet effet par la Commission, pourvus d'équipement informatique et accessible pendant les heures d'ouverture normale des bureaux (art. 63, b)

[202] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 296.

et 65). Enfin, une consultation indirecte est prévue, permettant de s'adresser à la CPVP, par écrit ou oralement en s'y présentant, afin de lui demander un extrait du registre public (art. 63, c) et 66), cet extrait pouvant être simplifié s'il concerne un grand nombre de traitements ou de responsables (art. 67).

C. Les compétences de la Commission

La CPVP est investie de diverses compétences, celles-ci demeurant peu novatrices et peu audacieuses, même après l'adoption de la directive européenne. En effet, si celle-ci élargit singulièrement les pouvoirs de l'autorité de contrôle, doublant ses pouvoirs d'investigation de pouvoirs effectifs d'intervention, y compris le "pouvoir d'ordonner l'effacement ou la destruction des données ou d'interdire temporairement ou définitivement un traitement" et du "pouvoir d'ester en justice", la loi belge ne semble pas avoir suivi le mouvement[203].

La première compétence attribuée à la Commission consiste une compétence d'**avis**. En effet, "la Commission émet soit d'initiative, soit sur demande du Gouvernement, des Chambres législatives, des Gouvernements de communauté ou de région, des Parlements de communauté ou de région, du Collège réuni ou de l'Assemblée réunie visés à l'article 60 de la loi spéciale du 12 janvier 1989 relative aux institutions bruxelloises ou d'un comité de surveillance, des avis sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel" (art. 29, § 1er). L'on voit que l'objet de cette compétence d'avis est très large, et dépasse les cas pour lesquels la loi impose cet avis, entre autres pour l'adoption d'arrêtés royaux. Ils peuvent en outre être pris d'initiative, une demande n'étant pas indispensable à l'exercice de cette compétence. Certaines exigences de forme et de délais sont prévues par l'article 29, lequel impose également, en son § 4, que les avis soient motivés. Le propre d'un avis est d'être non contraignant: il n'oblige pas la personne à qui il s'adresse à le suivre. Cela ne le prive toutefois pas de toute valeur, servant de guide à l'interprétation et à l'application de la loi. En outre, s'il est requis, il consiste en une exigence de forme substantielle, son absence entachant la décision qu'il doit accompagner d'illégalité. D'ailleurs, l'article 29, § 5 impose la publication de l'avis au Moniteur belge avec l'acte qu'il accompagne.

Un second chef de compétence reconnu à la CPVP consiste en **recommandations**, qu'elle peut adresser d'initiative ou à la demande des mêmes autorités qu'en cas d'avis, et qui portent sur le même objet que ceux-ci (art. 30). Elles doivent être motivées, tout comme la possibilité doit être offerte au responsable concerné de faire valoir son point de vue. Si l'avis s'adresse à une instance jouissant de pouvoirs législatifs, la recommandation concerne davantage un ou plusieurs responsables de traitements.

La troisième compétence reconnue à la CPVP lui permet d'**examiner les plaintes** qui lui sont adressées et qui peuvent avoir trait à "sa mission de protection de la vie privée à l'égard des traitements de données à caractère personnel ou à d'autres missions

[203] Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 393.

qui lui sont confiées par la loi" (art. 31). La loi et l'arrêté royal prévoient les règles de procédure, les conditions de recevabilité, les possibilités de médiations et les règles relatives aux décisions rendues.

Une compétence générale charge la CPVP de **veiller au respect de la loi**, compétence qui se concrétise par divers pouvoirs, à savoir un pouvoir d'enquête (art. 32, § 1er), un pouvoir de dénonciation en justice des infractions dont elle aurait connaissance (art. 32, § 2), ainsi que le pouvoir de réclamation reconnu au président de la Commission de soumettre au tribunal de première instance tout litige concernant l'application de la loi et de ses mesures d'exécution (art. 32, § 3). Ce dernier pouvoir offre à la CPVP un moyen de rendre contraignantes les décisions qu'elle prend[204]. Le tout sans préjudice de la compétence des cours et tribunaux.

S'ajoutent à ces quatre compétences principales un certain nombre de tâches relatives à l'application concrète de la loi, que celles-ci soient conférées à la CPVP par la loi elle-même – telles que par exemple l'exercice indirect de certains droits de la personne concernée, ou encore les tâches relatives aux déclarations et à la tenue du registre public - ou par l'arrêté d'exécution – concernant entre autres les traitements ultérieurs à des fins historiques, statistiques et scientifiques, ainsi que le traitement de catégories particulières de données à caractère personnel. En outre, diverses missions sont mises à charge de la Commission, comme celle qui consiste à établir un rapport d'activité annuel, ou encore celles dont le Roi peut la charger en vertu de l'article 32 *bis* en vue de l'application de conventions internationales.

Enfin, la CPVP est également investie de compétences par d'autres lois particulières, que ce soit des compétences d'avis ou des missions de collaboration avec certains comités de surveillance établis par ces lois[205].

D. Les règles de composition et de fonctionnement de la Commission

Nous n'entrerons pas dans les détails techniques des règles de composition – nomination, etc. – et de fonctionnement de la CPVP, qui est instituée auprès de la Chambre des Représentants, laquelle en désigne les membres, le président et le vice-président. Certaines informations se révèlent néanmoins pertinentes en la matière, et font l'objet d'un bref examen ci-dessous.

Tout d'abord, la CPVP doit être indépendante, et se membres doivent présenter un certain nombre de compétences, tout comme un équilibre technique, socio-économique et linguistique doit être maintenu entre ceux-ci. En outre les membres de la CPVP, ainsi que les experts dont elle peut requérir le concours sont "tenus d'une obligation de confidentialité à l'égard des faits, actes ou renseignements dont ils ont eu connaissance en raison de leurs fonctions"**.**

Quant au fonctionnement, il est établi par la CPVP elle-même, dans son règlement d'ordre intérieur. L'aspect le plus intéressant de ce fonctionnement réside dans la création de Comités sectoriels au sein de la Commission, "compétents pour instruire et statuer sur des demandes relatives au traitement ou à la communication de données faisant l'objet de

[204] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, p. 343.
[205] D. DE BOT, *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001, pp. 346-351.

législations particulières, dans les limites déterminées par celle-ci" (art. 31 *bis*, § 1er). C'est ainsi qu'a été créé en 2003 un Comité sectoriel pour l'autorité fédérale, et que depuis lors toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe de ce comité sectoriel, à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée. Existent en outre le Comité de surveillance statistique (AR du 7 juin 2007), ainsi que le Comité sectoriel de la sécurité sociale et de la santé, créé par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité Sociale. Selon le site officiel de la CPVP:

"Le Comité sectoriel de la Sécurité Sociale et de la Santé est quant à lui chargé de veiller au respect des lois et normes concernant la protection des données. Il lui appartient également d'autoriser le transfert de certaines informations d'un organisme à l'autre. Avant d'accorder une telle autorisation, le Comité sectoriel de la Sécurité Sociale et de la Santé demande à la Banque-Carrefour de lui remettre un avis juridique et technique.

La loi du 1er mars 2007 portant des dispositions diverses (III) a profondément modifié le fonctionnement et les compétences de la Banque-Carrefour et du Comité, particulièrement en ce qui concerne la communication et le traitement de données relatives à la santé.

Dorénavant, le traitement et la communication de telles données pourront être contrôlés par le Comité sectoriel de la Sécurité Sociale et de la Santé. Dans certains cas, la communication de données relatives à la santé ne pourra avoir lieu que si le Comité l'autorise au préalable.

Pour ce faire, l'ancien Comité sectoriel de la Sécurité Sociale a été transformé en un "Comité sectoriel de la Sécurité Sociale et de la Santé" composé de deux sections, respectivement compétentes en matière de sécurité sociale et de santé"[206].

[206] http://www.privacycommission.be.

Conclusion

La Belgique s'est dotée, le 8 décembre 1992, d'une loi visant à garantir la protection de la vie privée lors du traitement de données à caractère personnel, cette loi ayant été adaptée au fil des évolutions, notamment suite à la transposition de la directive européenne en la matière en 1999. L'importance d'une telle législation ne peut être démentie, des garanties légales étant essentielles en matière de protection de la vie privée. Toutefois, la loi belge contient diverses lacunes, imprécisions et autres inconvénients, que la doctrine, la jurisprudence et la Commission de la protection de la vie privée, entre autres, tentent de combler et de corriger.

S'agissant du sujet qui nous occupe dans le cadre du projet BeLHIS, plusieurs considérations peuvent être évoquées suite à l'analyse du cadre légal belge en matière de protection de la vie privée lors du traitement de données à caractère personnel. Tout d'abord, la loi sera plus que probablement applicable à tout traitement poursuivant une perspective longitudinale, pareille caractéristique excluant l'usage de données anonymisées. Il s'agira bel et bien de données à caractère personnel, pour le traitement desquelles la loi doit être respectée. De plus, il s'agira souvent de données relatives à la santé, ce qui implique qu'outre les conditions générales de licéité de tout traitement, des conditions spécifiques devront être respectées afin de pouvoir traiter ces données en toute légalité. Enfin, diverses obligations s'imposeront au responsable du traitement, que ce soit en matière de sécurité, de déclaration à la Commission de la protection de la vie privée, ou encore en vue de permettre aux personnes concernées d'exercer les droits que la loi leur reconnaît.

Il reste toutefois certains aspects que ce rapport n'envisage pas, certains problèmes qu'il ne permet pas de résoudre. En effet, en ce qui concerne les aspects véritablement techniques et concrets du traitement longitudinal de données à caractère personnel, l'analyse du cadre légal n'apporte que très peu d'informations, cette analyse s'intéressant davantage aux aspects juridiques de la question, et non à ses caractéristiques techniques. En outre, peu d'éclaircissements sont disponibles à l'égard du caractère longitudinal du traitement des données à caractère personnel, si ce n'est via certaines allusions évoquées de temps à autres. Tout ce qui concerne ces aspects longitudinaux à proprement parler reste donc encore à élucider.

Bibliographie

I. Législation

- L. 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, http://www.moniteur.be.
    - Projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, Commentaire des articles, *Doc. Parl.,* Ch. repr., sess. ord.1990-1991, n° 47K1610001 du 6 mai 1991, p. 11, http://www.lachambre.be.
    - Exposé des motifs, *Doc. parl.,* Ch. repr., sess. ord. 1997-1998, n° 1566/1.
    - Rapport au Roi par A.R. n° 14 du 22 mai 1996, *M.B.* 30 mai 1996, 14520.
    - Rapport fait au nom de la commission de la justice par Mme Merckx-Van Goey, *Doc. Parl.*, Ch. repr., sess. exrtr. 1991-1992, n° 413/012 du 2 juillet 1992, pp. 9-10, http://www.lachambre.be.
    -
- L. Du 4 juillet 1962 relative à la statistique publique, *M.B.*, 20 juillet 1962, http://www.moniteur.be.
- Arrêté royal du 13 février 2001portant 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, chapitre II, *M. B.,* 13 mars 2001, www.moniteur.be.
- Directive européenne 95/46/C.E. 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.,* L 281/31, 23 nov. 1995, http://www.eur-lex.europa.eu.
- Règlement (CE) n° 322/97 du conseil du 17 février 1997 relatif à la statistique communautaire, art. 13 à 18, *J.O.,* n° L 052 du 22 février 1997, pp. 0001/0007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997R0322:FR:HTML.
- Proposition de règlement du Parlement européen et du Conseil relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, 7 février 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007PC0046:FR:HTML.
- Recommandation n° R (97) 18F du 30 septembre 1997 du Comité des Ministres du Conseil de l'Europe aux Etats membres concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques, http://www.coe.int.
- Recommandation n° R (97) 5F du 13 février 1997 du Comité des Ministres du Conseil de l'Europe aux Etats membres relative à la protection des données médicales, p. 28, http://www.coe.int.
- Recommandation n° R (85) 20 du 25 octobre 1985 du Comité des Ministres du Conseil de l'Europe aux Etats membres relative à la protection des données à caractère personnel utilisées à des fins de marketing direct, http://www.coe.int.

- OECD Guidelines for the Security of Information Systems, 26 novembre 1992, http://www.oecd.org/document/19/0,3343,fr_2649_201185_1815059_1_1_1_1,00.html.

II. Doctrine

- BOULANGER, M.-H., CALLENS, S., et BRILLON, St., "La protection des données à caractère personnel relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001", *Rev. dr. Santé,* 2000-2001, p. 328.
- DE BOT, D., *Verwerking van persoonsgegevens,* Kluwer, Antwerpen, 2001.
- DE TERWANGNE, C., et LOUVEAUX, S., "Protection de la vie privée face au traitement des données à caractère personnel: le nouvel arrêté royal", *J.T.,* 2001, p. 465.
- LEONARD, Th., et POULLET, Y., "La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/C.E. du 24 octobre 1995, *J.T.*, 1999, p. 378.
- Avis 8/99 du 8 mars 1999 de la Commission de la protection de la vie privée, http://www.privacycommission.be.
- Avis n° 30/96 du 13 novembre 1996 de la Commission de la protection de la vie privée, http://www.privacycommission.be.
- Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME), adopté le 15 février 2007 par le Groupe de travail "ARTICLE 29" sur la protection des données, Commission européenne, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_fr.pdf.

DEUXIEME PARTIE

DEUX SUJETS D'ACTUALITE

Chapitre I[er]. – eHealth, la plate-forme électronique d'échange des données relatives à la santé

Ces derniers mois, la plate-forme eHealth d'échange électronique de données relatives à la santé figure à l'ordre du jour des activités politiques et parlementaires, tout comme elle fait l'objet de nombreux articles de presse. Ce projet, en germe depuis 2004, a pourtant connu quelques années de stagnation, avant de suivre une évolution des plus rapides et surprenantes, ce qui a suscité bon nombre de critiques ainsi qu'une réaction de méfiance dans le chef des acteurs du secteur de la santé. La bonne compréhension du projet requiert une brève présentation chronologique des étapes qu'il a connues, une analyse du texte du projet de loi ainsi qu'un examen des diverses réactions et justifications y apportées.

Section I[ère]. – Les origines: la plate-forme Be-Health

Jusqu'il y a peu, c'était sous le nom de Be-Health qu'était présentée la plate-forme d'échange électronique de données relatives à la santé, et qu'elle existait sous certaines formes. Certains aspects du projet eHealth trouvant leur source dans le projet Be-Health, il nous parait intéressant d'en évoquer les caractéristiques générales au cours des lignes qui suivent, avant d'entamer l'analyse du projet eHealth en tant que tel.

§ 1[er]. – De l'accord de principe à la création de la plate-forme Be-Health

Il semble que la longue élaboration de la plate-forme eHealth – dénommée à ses origines Be-Health – ait commencé en juillet 2004, lorsque le Conseil des Ministres accorda la permission d'organiser une première enquête et d'étudier les possibilités de cadre d'échange numérique de données médicales[207]. Une seconde note fut approuvée quelques mois plus tard, selon laquelle "le Conseil des Ministres a donné le feu vert pour la mise sur pied de Be-Health, une plate-forme au moyen de laquelle toutes les informations et applications du secteur des soins de santé seront offertes électroniquement via un site portail. Ce dernier donnera accès tant aux prestataires de soins de santé qu'aux patients"[208]. Une proposition concrète avait en effet été formulée le 20 décembre, prévoyant le budget, les finalités du projet, et la création d'un groupe Gestion ainsi que d'un groupe Vision.

Par la suite, et selon l'exposé de Mmes Van Nieuwkerke et Zriten retraçant à la Chambre des Représentants, en février 2006, les différentes étapes du projet Be-Health, l'architecture de base fut élaborée, les premiers tests furent effectués avec l'INAMI et le SPF Santé publique, le premier projet-pilote fut réalisé, des discussions furent menées au sein du groupe Vision, et d'autres projets-pilotes furent développés. Il était prévu pour

[207] Note du Conseil des Ministres du 20 juillet 2004.
[208] Centre de presse international relatif au Conseil des Ministres du 23 décembre 2004, http://www.belgium.be/eportal/application?languageParameter=fr&pageid=contentPage&docId=37478.

2006 d'examiner le cadre légal dans lequel la plate-forme de services Be-Health devait s'inscrire[209]. Entre temps, le projet avait été évoqué à plusieurs reprises au sein des assemblées parlementaires.

Tout d'abord, en octobre 2005, il fut déclaré au Sénat[210] que la stratégie de développement des soins de santé par voie électronique s'appuie sur trois chantiers réglementaires, prioritaires et complémentaires, à savoir:

- Renforcer la confidentialité des données de santé et sa maîtrise:
  - Définition des données de santé;
  - Création d'un numéro d'identification de santé personnel;
  - Création, au sein de la Commission de la protection de la vie privée, d'un comité sectoriel pour les données de santé (aujourd'hui devenu Comité sectoriel de la sécurité sociale et de la santé, mais dont la section santé n'a pas encore été créée à ce jour).
- Fixer les règles et standards pour garantir la sécurité et l'interopérabilité des logiciels pour le dossier médical et pour les applications télémédicales.
- Mettre en place une plate-forme télématique d'accès commun.

Au cours des débats parlementaires, l'attention fut attirée sur l'importance de différencier le projet Be-Health du projet de loi relatif aux données de santé et à leur informatisation, tout comme certains éclaircissements sont apportés au sujet du groupe Vision, dont la mise en place est une conséquence du démarrage du projet Be-Health. Ce groupe est responsable de la définition et de la mise à jour de la vision du projet Be-Health, en concertation avec les Commissions et les Associations représentatives des utilisateurs. Ce groupe fut instauré le 2 décembre 2005, et est consulté quant aux objectifs et à l'évolution du projet de loi relatif aux données de santé et à leur informatisation, avant la communication du texte à la Commission de la vie privée.

Le 8 novembre 2005, le Ministre des Affaires sociales et de Santé publique répondait à la question de Guy D'Haeseleer, concernant l'état d'avancement du projet Be-Health[211]. Après avoir énoncé les divers avantages et risques de l'*e-health* – les principaux risques relevant de la protection de la vie privée –, le Ministre affirma la nécessité de développer une stratégie nationale, laquelle serait mise en place par un projet de loi.

Différentes étapes étaient prévues pour ce faire:

- Concertation au sein d'un groupe d'utilisateurs, à savoir le groupe Vision;
- Demande d'avis à la Commission de la protection de la vie privée;
- Demande d'avis à l'Ordre des médecins et aux syndicats médicaux;
- Présentation du projet au Conseil des Ministres;
- Demande d'avis au Conseil d'Etat;
- Dépôt du projet au Parlement.

---

[209] Proposition de résolution visant à soutenir les facteurs critiques de succès nécessaires à la réussite de l'e-société, amendement n°19 proposé par M. Van Nieuwkerke et Mme Zriten le 20 février 2006, *Doc. Parl.,* Ch. repr., sess. ord., 2005-2006, www.lachambre.be.

[210] Question n° 3-3666 de Mme Annemie VAN DE CASTEELE du 28 octobre 2005 (N), *Bull.Q. R.,* Sén., sess. ord. 2005-2006, n° 3-53, http://www.senat.be.

[211] Réponse du Ministre des Affaires sociales et de Santé publique du 8 novembre 2005, à la question n° 489 de M. Guy D'HAESELEER, du 14 juin 2005 (N), *Bull. Q. R.,* Ch. repr., sess. ord. 2005-2006, n° 099, pp.18006-18010, www.lachambre.be.

Le projet de loi comportera:

- La création d'un comité sectoriel propre aux données de santé, au sein de la Commission de la vie privée;
- La création d'une plate-forme "Be-Health";
- La création d'un identifiant personnel de santé, différent du numéro d'identification de la sécurité sociale (NISS);
- La création du dossier de santé partagé;
- La définition de certaines applications de télémédecine, à savoir la téléconsultance entre médecins, le télémonitoring et la prescription électronique;
- L'imposition de règles de sécurité, afin de garantir principalement la protection de la vie privée.

Cette évolution s'acheva par l'adoption de la loi du 27 décembre 2006[212] portant dispositions diverses, qui prévoit, en son article 4, la création d'un service de l'Etat à gestion séparée, dénommé Be-Health, au sein du SPF Santé publique, Sécurité de la Chaîne alimentaire et Environnement, en vue de la gestion de la plate-forme électronique de services relative à l'échange de données de soins de santé. La loi charge le Roi de déterminer, par arrêté royal, les missions et modalités de gestion et d'exploitation de ce service de l'Etat à gestion séparée. Il semble toutefois que cet arrêté royal n'ait jamais été adopté.

§ 2. – Fonctionnement et applications de la plate-forme Be-Health

Actuellement, c'est toujours sous le nom de Be-Health que la plate-forme existe, sous l'adresse internet www.behealth.be. Elle comporte plusieurs applications, la principale étant celle de la Fondation Registre du cancer, que nous détaillerons ci-dessous, après avoir brièvement expliqué le fonctionnement de la plate-forme.

A. Accès limité et respect de la vie privée

L'accès aux applications prévues par la plate-forme Be-Health est conditionné à une identification, soit via un token, c'est-à-dire un numéro comportant 24 chiffres – procédure semblable à celle suivie par les banques pour l'utilisation des *digipass* –, soit via la carte d'identité électronique. Différents types d'accès sont prévus, deux d'entre eux ne comportant encore aucune application, à savoir les accès "citoyen" et "entreprise". L'accès "professionnel" contient différentes rubriques telles que accoucheuse, dentiste, diététicien, ou encore logopède; tout comme c'est le cas de l'accès "groupements et institutions" qui se subdivise en "hôpital général", "hôpital psychiatrique", "maison de

[212] L. du 27 décembre 2006 portant dispositions diverses (I), *M.B.,* 28 décembre 2006, art. 4, http://www.moniteur.be.

[7] Ce règlement est disponible à la page suivante: https://www.behealth.be/behealth/content/fr/common/body/pdf/users_F.pdf.

repos", etc. Chaque médecin ou institution valablement identifié dispose de l'accès aux applications qu'il est autorisé à utiliser.

Le "Règlement à l'usage des utilisateurs en vue de l'accès et de l'utilisation du système informatique de l'Etat fédéral et des institutions publiques de sécurité sociale par les entreprises et leurs mandataires"[213] précise en effet que différents accès sont prévus pour différentes personnes, certaines applications étant accessibles à tous les utilisateurs, d'autres se limitant à certains d'entre eux. Chaque utilisateur reçoit un nom d'utilisateur et un mot de passe, qui sont strictement personnels et intransmissibles. Ils sont attribués aux gestionnaires locaux par Eranova, Centre de Contact des institutions publiques de sécurité sociale, et aux autres utilisateurs par le gestionnaire local d'une entreprise. Chaque utilisateur est responsable de l'usage approprié ou non qu'il en fait. Ce règlement mentionne également l'obligation de fournir des informations complètes, exactes et véritables, de respecter les prescriptions légales et réglementaires, ainsi que de s'abstenir de manipuler les informations fournies. Enfin, l'accès à certains services est soumis à une réglementation plus stricte, requérant entre autres une clé privée ainsi qu'un certificat.

En ce qui concerne les personnes physiques, les entreprises et les groupements infirmiers, un système de mandats est prévu. Ceux-ci peuvent être accordés aux personnes visées, par un professionnel ou une institution jouissant de l'accès à certaines applications, pour une application précise, et pour une durée déterminée ou indéterminée. La personne qui a obtenu un mandat pourra donc utiliser Be-Health pour l'application pour laquelle le mandat lui a été conféré. Elle devra donc s'identifier comme les autres utilisateurs de la plate-forme.

S'agissant de la protection de la vie privée, un certain nombre de règles sont énoncées sur le site internet lui-même, en ces termes:

"La Direction générale de la Communication Externe, au sein du Service public fédéral (SPF) Chancellerie du Premier Ministre respecte la vie privée des utilisateurs. Bien que la plupart des informations soient disponibles sur ce site sans devoir fournir des données à caractère personnel, il est possible que des informations personnelles soient demandées à l'utilisateur. Dans ce cas, les données sont traitées conformément aux dispositions de la loi du 8 décembre 1992 relative au traitement de données à caractère personnel. Concrètement, cela signifie notamment que:

- *les données à caractère personnel ne peuvent être recueillies et traitées que dans le but de répondre à la demande d'information que vous avez introduite ;*
- *les données à caractère personnel ne seront pas communiquées à des tiers ni utilisées à des fins commerciales ;*
- *vous avez le droit de consulter vos données personnelles et que vous pouvez vérifier leur exactitude et faire corriger les éventuelles erreurs les concernant. A cet effet, vous pouvez prendre contact avec le gestionnaire du site.*

La Direction générale de la Communication Externe s'engage à prendre les meilleures mesures de sécurité afin d'éviter que des tiers n'abusent des données à caractère personnel que vous avez communiquées"[214].

---

[214] https://www.behealth.be/behealth/goTo.do?privacy.action.

B. L'application Registre du Cancer

L'une des applications présentes sur le site de Be-Health permet l'enregistrement en ligne de données relatives au cancer[215]. En effet, tous les hôpitaux doivent, depuis 2003, communiquer à la Fondation Registre du Cancer (FRC) certaines données sur le cancer, mais ils choisissent de le faire soit par l'envoi annuel de lots de badges, soit via le portail Be-Health, système de saisie en ligne mis au point en 2006 et avec lequel la FRC collabore depuis 2007. Pour ceux qui optent pour l'utilisation de Be-Health, la direction de l'hôpital désigne un gestionnaire local, qui fait office de personne de contact, représentant l'hôpital tout au long de la procédure. Les médecins autorisés à utiliser Be-Health sont également désignés, ayant seuls accès au portail afin d'y enregistrer les données qu'ils possèdent. Toute utilisation du portail nécessite au préalable une procédure de vérification et d'identification, laquelle consiste en la vérification de plusieurs informations, à savoir: l'identité du médecin, via sa carte d'identité électronique ou son code token, son numéro INAMI, le fait qu'il ait été déclaré par le gestionnaire local comme utilisateur, et enfin les droits qui lui ont été conférés par le gestionnaire local – en effet, rappelons qu'il existe différents types d'accès et d'utilisations. Les médecins valablement identifiés ont donc accès à l'application Registre du Cancer. Ils enregistrent en ligne leurs données et n'ont accès qu'à leurs propres données. Un médecin coordinateur par hôpital a accès à toutes les données de son hôpital, afin de pouvoir établir les statistiques propres à cet hôpital.

Cela permet à la FRC de travailler sur base des données qui ont été enregistrées par les médecins sur le portail Be-Health. Avant, un système de certificats d'une société privée était mis en œuvre, mais la procédure de vérification de chaque médecin pour chaque hôpital était trop compliquée, raison pour laquelle l'usage de la plate-forme Be-Health a été favorisé. Le site précise que "les données administratives des patients sont téléchargées lors de l'introduction de leur NISS. Les données médicales sont ensuite encodées d'après les codifications internationales (TNM,ICD-O3)"[216]. Précisons en effet que la FRC est autorisée à utiliser le numéro du registre national – qui est le même que le NISS – ainsi que nous le détaillons dans le chapitre concernant l'utilisation de ce numéro.

C. Autres applications

L'application Registre du Cancer n'est pas la seule à avoir été mise en ligne. En effet, l'application eShop permet de commander en ligne des attestations de soins donnés, telles que des carnets, formules en continu et vignettes de concordance. Une autre application, dénommée SAFE (Shared Artritis File for Electronic Use), facilite l'enregistrement de données administratives et médicales dans le cadre du traitement de la polyarthrite rhumatoïde. Les rhumatologues y introduisent des données médicales dans un but de suivi de l'évolution du patient et des conditions de prescription. S'ajoute à cela l'application MyCareNet, qui concerne la question de l'assurabilité, et qui vise à optimaliser et à simplifier la circulation de l'information entre les prestataires de soins et

[215] Les informations présentées ici au sujet de l'application Registre du Cancer ont été recueillies au cours d'une conversation téléphonique avec une personne travaillant à la Fondation Registre du Cancer.
[216] https://www.behealth.be/behealth/goTo.do?sva.action&service=rc.

les mutualités, par le biais d'un échange électronique et sécurisé de données au travers d'une plate-forme Internet. Enfin, d'autres utilisations de Be-Health sont en projet, telles que l'enregistrement des naissances, ou encore les commandes de matériel.

Section II. – Le projet eHealth

Aujourd'hui, c'est sans son "B" que la plate-forme électronique d'échange des données de santé fait partie des sujets d'actualité. En quelques mois, le projet de loi a vu le jour puis a été adopté par les deux assemblées parlementaires, tout en étant loin d'être approuvé par tous les acteurs du secteur de santé concernés. Nous analyserons les différentes justifications d'une part, ainsi que les critiques adressées au projet, d'autre part, après avoir brièvement retracé l'évolution rapide qu'a connu ce projet.

§ 1er. – Un projet prioritaire

Si depuis la loi de 2006 le projet Be-Health est relativement resté dans l'ombre, son évolution paraissant en quelque sorte stagnante, les choses se sont quelque peu précipitées depuis le mois de mars 2008. En effet, le Conseil des Ministres du 7 mars approuva, de manière plutôt inattendue et relativement surprenante, un avant-projet de loi relatif à la constitution et à l'organisation de la plate-forme eHealth[217]. Un mois plus tard à peine, la Commission de la protection de la vie privée (CPVP) rendait un avis[218] favorable concernant ce projet, tout comme le Conseil d'Etat se prononça en faveur de celui-ci, moyennant certaines précisions[219]. Au moment de son dépôt à la Chambre des Représentants, le projet eHealth était inclus dans un projet de loi "fourre-tout", à savoir le projet de loi portant dispositions diverses (I)[220], dont les chapitre 3 et 4 du titre X traitaient de l'institution et de l'organisation de la plate-forme eHealth. Suite à de nombreuses contestations, émanant principalement de l'ABSyM (Association belge des syndicats médicaux)[221] et du Conseil National de l'Ordre des médecins[222], réclamant qu'un débat parlementaire soit tenu à ce sujet, la Ministre des Affaires sociales Laurette

[217] Communiqué du Conseil des Ministres du 7 mars 2008, http://socialsecurity.fgov.be/fr/nieuws_publicaties/nieuwsoverzicht/2008/03.htm#35222; ou www.stomie.be/fra/acc_actu.php?art=1411.

[218] Avis de la Commission de la protection de la vie privée n° 14/2008 du 2 avril 2008, à la demande de la Ministre des Affaires sociales et de la Santé publique et de la Ministre de la Fonction publique et des Entreprises publiques concernant un projet de loi portant institution et organisation de la plate-forme eHealth (A/2008/016), http://www.privacycommission.be/fr/docs/Commission/2008/avis_14_2008.pdf.

[219] Avis du Conseil d'Etat n° 44.351/1/2/3/4, joint au projet de loi portant dispositions diverses (I), déposé à la Chambre des Représentants le 29 mai 2008, Doc. 52 1200/001, http://www.lachambre.be/FLWB/PDF/52/1200/52K1200001.pdf.

[220] Projet de loi portant dispositions diverses (I), déposé à la Chambre des Représentants le 29 mai 2008, Doc. n° 52 1200/001, http://www.lachambre.be/FLWB/PDF/52/1200/52K1200001.pdf.

[221] [221] http://fr.medisurf.be/protected/archives/WebTV/Archief/20080610.html.

[222] Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html.

Onkelinx accepta de faire du projet eHealth un projet de loi à part entière[223]. Selon la Ministre, "cela laissera davantage de temps pour permettre les auditions de la CPVP et du Conseil national de l'Ordre des médecins", l'objectif étant "d'organiser un débat totalement transparent et d'éviter les fantasmes basés sur la première mouture du dossier"[224].

Cependant, il semble que ce débat ait été faussé et précipité, ne laissant aux principaux concernés que très peu de temps pour réagir. En effet, la Chambre des Représentants adopta le projet de loi en moins d'un mois, après trois séances en Commission de la Santé Publique, par 101 voix, 0 non et 34 abstentions. Le Sénat usa certes de son droit d'évocation, mais sans grande utilité, décidant en une semaine à peine de ne pas amender le texte tel qu'adopté par la Chambre. Le parti écolo dénonce d'ailleurs cette précipitation qu'il qualifie d'irresponsable, incompréhensible et inefficace": "Une après-midi d'auditions, trois jours pour déposer les amendements, et puis débat et vote au pas de charge en Commission santé de la Chambre pour ensuite l'adopter en plénière tout aussi promptement… Les écologistes sont les seuls partis démocratiques à s'être abstenus"[225]. Quoi qu'il en soit, et malgré les contestations persistantes ainsi que les reproches adressés au projet tenant au manque de concertation des acteurs du secteur de santé, le Sénat a adopté le projet le 18 juillet 2008 sans modifications, par 40 voix contre 4 et aucune abstention. Le projet est donc transmis à la Chambre des Représentants en vue de la sanction royale[226].

§ 2. – Présentation du contenu du projet de loi

Mis à part l'abandon du "B" et l'abrogation de toutes les dispositions légales concernant la plate-forme Be-Health – puisqu'eHealth est amenée à la remplacer –, le projet de loi apporte bon nombre de modifications à la loi de 2006 qui a institué Be-Health.

A. Une institution publique dotée de la personnalité juridique, au sein de la Banque Carrefour de la Sécurité Sociale

Une première et importante modification concerne le statut de la plate-forme. Il ne s'agit plus de créer un service d'Etat à gestion séparée, comme l'article 4 de la loi du 27 décembre 2006 le faisait, mais bien d'une institution publique dotée de la personnalité juridique. De plus, cette institution est à créer au sein de la Banque Carrefour de la

---

[223] Projet de loi relative à l'institution et à l'organisation de la plate-forme eHealth, déposé à la Chambre des Représentants le 17 juin 2008, Doc. n° Doc 52 1257/001, http://www.lachambre.be/FLWB/PDF/52/1257/52K1257001.pdf. Ce document a, avant le débat et les amendements, exactement le même contenu que les chapitres du projet de loi portant dispositions diverses relatifs à la plate-forme eHealth.

[224] Le Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/77dd60ff-534e-42d0-b47c-1ba391f29cfa.vak.html.

[225] Le Journal du Médecin n° 1932 du 25 juillet 2008, p. 1, http://www.magazines.medisurf.be/AK1932/akmagazine.aspx?language=fr.

[226] http://www.senate.be/www/?MIval=/index_senate&MENUID=21200&LANG=fr.

Sécurité Sociale (BCSS), contrairement à Be-Health qui est intégrée au Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement. L'exposé des motifs explique les raisons de ce changement.

Lors de l'adoption des arrêtés d'exécution de l'article 4 de la loi du 27 décembre 2006, ces textes étant soumis pour avis au Conseil d'Etat, celui-ci avait "fait remarquer que les missions qui seraient attribuées à la plate-forme eHealth dépassent les missions qui sont normalement confiées à un service à gestion séparée et que l'organisation prévue, avec un comité de gestion composé de représentants des acteurs des soins de santé, correspond plutôt à l'organisation d'une institution publique dotée de la personnalité juridique". Le texte ajoute que la plate-forme eHealth est considérée comme une institution publique de sécurité sociale, ce qui la soumet aux règles s'appliquant à ce type d'institution. Cette forme juridique est, selon l'exposé des motifs, la plus appropriée pour la plate-forme eHealth. Il en découle qu'elle disposera d'un Comité de gestion propre, composé de représentants des diverses parties intéressées du secteur des soins de santé, ainsi que de ressources financières propres. En outre, les règles et conditions d'exécution de ses missions légales seront fixées dans un contrat d'administration, conclu entre eHealth et l'Etat, les ministres de tutelle étant en l'espère ceux compétents pour la Santé publique, les Affaires sociales et l'Informatisation de l'Etat, le Comité de gestion assumant quant à lui le rôle d'organe de gestion pour ce contrat d'administration.

S'agissant de l'intégration de la plate-forme au sein de la BCSS, c'est entre autres afin de bénéficier du *know-how* de celle-ci qu'elle est justifiée. Il s'agit de permettre à eHealth de bénéficier des services de base développés par la BCSS, la réutilisation de ce qui existe déjà étant ici promue. Ainsi que nous le verrons ci-dessous, la gestion journalière de la plate-forme sera confiée à l'administrateur de la BCSS, à savoir F. Robben, et ce dans le but de garantir une certaine unité en termes de direction.

B. Les objectifs de la plate-forme eHealth

Le projet de loi, en son article 5, octroie trois objectifs à la plate-forme eHealth, le premier étant d'optimaliser la qualité et la continuité des prestations de soins de santé, ainsi que la sécurité du patient. Selon la Ministre Onkelinx, "un échange électronique mutuel bien organisé d'informations significatives relatives au patient, aux soins administrés et aux résultats des soins administrés qui sont disponibles auprès des différents prestataires de soins et établissements de soins concernant un patient donné peut augmenter, de manière substantielle, la qualité des soins et la sécurité des patients"[227].

Le second but assigné à la plate-forme tient à promouvoir la simplification des formalités administratives pour tous les acteurs des soins de santé, dont entre autres les prestataires et établissements de soins. La Ministre des Affaires sociales justifie cet objectif en ces termes: "Grâce à des processus électroniques bien organisés et à l'accès à certaines banques de données, les prestataires de soins et les établissements de soins

[227] Rapport fait au nom de la Commission des Affaires sociales par M. Brotchi, Sénat, Doc. n° 4-863/2, file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/rapport%20commission%20affaires%20sociales%20S%C3%A9nat.htm.

peuvent être déchargés de nombreuses formalités administratives, de sorte qu'ils peuvent consacrer davantage de temps à leurs patients et à leur formation continue. Les pays où un projet similaire se trouve déjà à un stade fort avancé font état d'un gain de temps de 15 % pour les prestataires de soins. Les patients pourront aussi bénéficier de délais d'attente plus brefs pour l'administration de certains soins, étant donné qu'il ne faudra plus parcourir des procédures papier en vue d'obtenir l'autorisation pour l'administration de certains soins ou en vue de la transmission d'informations"[228].

Enfin, il s'agit également de soutenir la politique en matière de santé, laquelle doit, toujours selon la Ministre, se fonder sur des études et analyses solides. "A cet effet, il est nécessaire, en fonction de la finalité — par exemple le suivi longitudinal ou non des patients atteints de différentes pathologies — de disposer d'informations actuelles, anonymisées ou codées, relatives aux patients et à leur état de santé, aux soins administrés et aux résultats des soins administrés. Ces informations anonymes ou codées doivent pouvoir être utilisées en vue de la préparation et de l'évaluation de la politique des soins de santé par les diverses instances compétentes, tout en offrant des garanties absolues au niveau de la protection de la vie privée des patients"[229].

Sous la section consacrée aux objectifs de la plate-forme, l'exposé des motifs précise qu'eHealth a "uniquement une fonction de prestation de services et d'appui pour les divers acteurs des soins de santé, sans qu'elle ne puisse intervenir dans les processus décisionnels des soins de santé". Cela a pour conséquence qu'aucune modification n'est apportée à la répartition des tâches et des compétences existante entre les acteurs des soins de santé, chacun d'entre eux conservant l'intégralité de ses compétences. En outre, il ne s'agit pas d'organiser un enregistrement central de données à caractère personnel, mais bien de procurer une infrastructure pour le soutien de l'échange de données électronique sécurisé entre les divers acteurs. La mission de l'enregistrement des données reste confiée à ces derniers. Enfin, l'exposé des motifs insiste sur le fait qu'eHealth n'obtiendra pas de monopole concernant les divers services qu'elle offrira, la possibilité restant offerte à d'autres instances de fournir pareils services.

C. Les missions de la plate-forme eHealth

L'article 5 confie dix missions à la plate-forme eHealth, la première étant celle de "développer une vision et une stratégie pour une prestation de services et un échange d'informations électroniques dans les soins de santé efficaces, effectifs et dûment sécurisés, tout en respectant la protection de la vie privée et en concertation étroite avec les divers acteurs publics et privés des soins de santé" (art. 5, 1°). C'est également à eHealth que revient la tâche de promouvoir le respect de cette vision et de cette stratégie (art. 5, 9°). Il s'agit là de la philosophie générale du projet.

---

[228] Rapport fait au nom de la Commission des Affaires sociales par M. Brotchi, Sénat, Doc. n° 4-863/2, file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/rapport%20commission%20affaires%20sociales%20S%C3%A9nat.htm.

[229] Rapport fait au nom de la Commission des Affaires sociales par M. Brotchi, Sénat, Doc. n° 4-863/2, file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/rapport%20commission%20affaires%20sociales%20S%C3%A9nat.htm.

Deux autres missions sont davantage d'ordre technique, concernant la détermination des normes, standards et spécifications TIC fonctionnels et techniques, ainsi que la vérification de la conformité des logiciels de gestion des dossiers électroniques de patients à ces normes (art. 5, 2° et 3°). L'exposé des motifs précise toutefois qu'il ne s'agit nullement pour eHealth de fixer des normes juridiques ou d'intervenir dans les processus décisionnels des soins de santé. De plus, si la plate-forme assure l'enregistrement des logiciels dont il est question, aucune mission de reconnaissance préalable de ceux-ci ne lui est attribuée, de sorte qu'aucune limitation n'est apportée au libre accès au marché dans le chef des fournisseurs de ces logiciels. Une autre mission est relativement proche de celles-ci, consistant en la gestion et la coordination des aspects TIC organisationnels, fonctionnels et techniques de l'échange de données à caractère personnel dans le cadre des dossiers électroniques de patients et des prescriptions médicales électroniques (art. 5, 7°).

Une quatrième mission vise les services électroniques qu'eHealth doit concevoir, gérer et développer en vue d'aider les acteurs des soins de santé. Il s'agit, selon l'exposé des motifs, "d'orchestrer les processus électroniques et de prévoir un environnement portail (comprenant notamment un système de gestion de contenu et un moteur de recherche) ainsi qu'un système de logging pour l'échange électronique de données à caractère personnel, en vue du traitement de plaintes éventuelles et de la détection d'irrégularités éventuelles" (art. 5, 4°, a)). En outre, la plate-forme développera et offrira des services de base tels qu'un système de gestion des accès et des utilisateurs, une boîte aux lettres électronique sécurisée pour chaque acteur des soins de santé, un système de datage électronique, un système de codage et d'anonymisation des informations, ou encore un répertoire de références indiquant, avec l'accord des patients concernés, auprès de quels acteurs des soins de santé sont conservés quels types de données pour quels patients (art. 5, 4°, b)). Rappelons que ce répertoire de référence ne consiste nullement en un enregistrement centralisé des données à caractère personnel, celles-ci n'étant pas enregistrées au sein de la plate-forme eHealth.

Afin d'éviter une centralisation inutile, des menaces inutiles pour la protection de la vie privée ainsi que des contrôles identiques et des enregistrements de loggings multiples, la mission de décider d'une répartition des tâches fonctionnelle décentralisée est confiée à la plate-forme, et ce dans le but de déterminer quel acteur des soins de santé enregistre quelles données à caractère personnel dans des sources authentiques validées, les gère et les rend accessibles. Notons cependant que l'article 5, 5° n'octroie aucune compétence normative en la matière à eHealth.

La plate-forme est en outre chargée de promouvoir et de coordonner des projets et programmes – au sens d'ensembles intégrés de projets et non de programmes informatiques – concernant plusieurs acteurs, à partir d'une approche multidisciplinaire (art. 5, 6°).

Afin d'assurer une mission relativement contestée, ainsi que nous le verrons ci-dessous, la plate-forme eHealth agit en tant qu'organisme intermédiaire au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée et de son arrêté d'exécution, pour l'agrégation et le codage ou l'anonymisation de données à caractère personnel pertinentes à des fins historiques, statistiques ou scientifiques (art. 5, 8°). Cette mission a pour but de permettre une aide à la recherche scientifique, puisque le résultat peut être mis à disposition des destinataires qui procèderont au traitement à des fins historiques,

statistiques ou scientifiques. Cela signifie, selon l'exposé des motifs, que la plate-forme peut prêter sa collaboration à des études scientifiques et d'appui à la politique en matière de soins de santé, mais qu'elle ne peut pour autant procéder elle-même à la réalisation de telles études, remplissant uniquement une fonction de prestation de services. Si le projet de loi précise qu'eHealth peut conserver des tableaux de concordance indiquant le lien entre les données codées et l'identité de la personne à laquelle elles ont trait, il ajoute cependant qu'elle ne peut le faire que lorsque le destinataire des données à caractère personnel codées le demande explicitement et de manière motivée. L'exposé des motifs cite à titre d'exemple le cas d'une étude longitudinale, pour la réalisation de laquelle les mêmes personnes doivent être suivies pendant une période plus longue, ce qui nécessite qu'elles puissent être identifiées. La plate-forme ne peut faire droit à cette demande que moyennant une autorisation de la section santé du comité sectoriel de la sécurité sociale et de la santé. Ces garanties ont été spécifiées dans le projet de loi lui-même sur proposition de la CPVP, dans son avis que nous examinerons au cours du § 3 de cette section.

Enfin, l'article 5, 10° appelle la plate-forme à collaborer avec d'autres instances publiques, tous niveaux de pouvoir confondus, en vue d'une prestation de services cohérente, intégrée, consistante et axée sur les utilisateurs finaux. Il s'agit entre autres, selon l'exposé des motifs, de collaborer avec la BCSS, le SPF Technologies de l'information et de la communication, la Coördinatiecel Vlaams e-gouvernement (CORVE), ou encore son pendant wallon (EASI-WAL).

D. Les droits et obligations de la plate-forme eHealth

1. Le respect de la protection de la vie privée et des droits du patient

L'article 6 de la loi précise d'emblée que le projet eHealth ne peut porter atteinte à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, pas plus qu'à la loi du 22 août 2002 relative aux droits du patient. C'est la CPVP qui a suggéré d'insérer cette disposition, en raison de l'importance de la confiance que les usagers doivent avoir en eHealth. Une garantie légale du respect de la protection de la vie privée et des droits du patient est de la sorte offerte, même si elle peut paraître relativement vide de contenu.

2. L'utilisation du numéro du registre national des personnes physiques et l'accès à celui-ci

Les deux articles suivants sont quelque peu plus surprenants, témoignant d'un revirement de jurisprudence de la CPVP, revirement que nous analyserons en détail lors de l'examen de l'avis de la CPVP. En effet, la plate-forme eHealth a non seulement accès aux données enregistrées dans le Registre national des personnes physiques, mais elle est en outre autorisée à utiliser le numéro d'identification de ce registre. Il s'agit donc de données à caractère personnel, y compris le numéro d'identification, qui peuvent notamment être utilisées dans le cadre de la gestion des accès et des utilisateurs appliquée

par la plate-forme eHealth[230]. L'exposé des motifs précise que, pour les personnes qui ne disposent pas ou pas encore d'un numéro d'identification du Registre national, eHealth peut utiliser le numéro attribué à ces personnes par la BCSS en application de la loi ayant créé cette institution[231]. Le texte précise également que la plate-forme a accès aux banques de données à caractère personnel gérées par la BCSS, lesquelles sont complémentaires et subsidiaires par rapport au Registre national étant donné qu'elles contiennent des données d'identification de base relatives aux personnes qui ne sont pas inscrites au Registre national ou dont les données ne sont plus systématiquement mises à jour dans ce registre. Cet accès est toutefois conditionné à l'octroi d'une autorisation de principe du comité sectoriel de la sécurité sociale et de la santé.

Au-delà du droit d'utiliser le numéro d'identification du registre national, le projet de loi impose même l'utilisation de ce numéro "lors de la communication de données à caractère personnel non codées à ou par la plate-forme eHealth" (art. 8). Ainsi, lors des échanges de données à caractère personnel se déroulant à l'intervention de la plate-forme eHealth, seul ce numéro pourra être utilisé – ou le numéro octroyé par la BCSS, le cas échéant. L'exposé des motifs justifie cette disposition de la sorte: "L'utilisation d'une clé d'identification unique offre des garanties pour une identification correcte des intéressés à chaque stade de l'échange de données à caractère personnel, c'est-à-dire tant pour l'émetteur que pour le destinataire des données à caractère personnel et pour les éventuels autres intervenants"[232]. De plus, il est précisé que cette l'obligation d'utiliser ces numéros d'identification ne concerne que l'échange de données à caractère personnel à l'intervention de la plate-forme eHealth, les acteurs des soins de santé demeurant libres de continuer à utiliser leur propre système d'identification pour d'autres finalités internes.

Au cours des débats parlementaires, M. Bart Van den Bosch, directeur des systèmes d'information des *Universitaire Ziekenhuizen* de Leuven, s'est prononcé en faveur de l'utilisation du numéro du registre national plutôt que de créer un numéro spécifique au secteur de la santé, arguments à l'appui[233].

La promotion de l'usage du numéro d'identification du registre national parait surprenante à première vue, étant donné qu'auparavant c'était la création d'un numéro spécifique au secteur de la santé qui était favorisée. Nous analyserons ce changement de vue ainsi que la justification qu'y apporte la CPVP au cours du troisième paragraphe de cette section/ du chapitre consacré à l'utilisation du numéro du registre national et à la jurisprudence de la CPVP à ce sujet.

3. *Les mesures de sécurité*

Le projet de loi contient diverses dispositions visant à assurer la protection de la vie privée ainsi que la sécurité des échanges de données à caractère personnel. Tout d'abord, un conseiller en sécurité de l'information doit être désigné par la plate-forme eHealth, parmi les membres de son personnel et après avis de la section santé du comité

[230] Exposé des motifs, art. 128.
[231] L. du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, art. 8, § 1er, 2°, *M.B.,* 22 février 1990, www.moniteur.be.
[232] Exposé des motifs, art. 129.
[233] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 35-36, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

sectoriel. Ce conseiller doit disposer, selon l'exposé des motifs, de l'indépendance et de l'expertise nécessaires à la correcte réalisation de sa mission. Celle-ci consiste en la surveillance des traitements et des échanges de données à caractère personnel réalisés par eHealth, en accordant une attention particulière à la protection de la vie privée des personnes auxquelles ces données ont trait. Pour ce faire, la loi charge le conseiller en sécurité de l'information de "fournir des avis qualifiés à la personne chargée de la gestion journalière" (art. 9, § 2, 1°), ainsi que "d'exécuter d'autres missions qui lui sont confiées par la personne chargée de la gestion journalière" (art. 9, § 2, 2°). Des règles particulières peuvent en outre être fixées par arrêté royal, concernant l'exécution de la mission, les compétences, l'indépendance et la responsabilité du conseiller en sécurité de l'information. Selon l'exposé des motifs, cette obligation souligne l'importance attachée à la protection de la vie privée. L'on peut toutefois comprendre que cette disposition ne rassure que très peu les opposants au projet eHealth, le conseiller en sécurité de l'information semblant bien soumis à la personne chargée de la gestion journalière, à savoir F. Robben, qui est l'administrateur général de la BCSS tout en étant présent dans diverses institutions de sécurité sociale, ainsi qu'à la CPVP.

L'article 10 prévoit une mesure de sécurité supplémentaire, tenant en l'obligation dans le chef du comité de gestion de désigner un médecin sous la surveillance et la responsabilité duquel s'effectue le traitement de données à caractère personnel relatives à la santé par la plate-forme eHealth. Ce médecin, tout comme le conseiller en sécurité de l'information, doit être désigné parmi les membres du personnel de la plate-forme, et après avis de la section santé du comité sectoriel. Une fois de plus, des règles de compétence, d'indépendance et de responsabilité peuvent être fixées par arrêté royal.

4. *L'autorisation de principe de la section santé du comité sectoriel de la sécurité sociale et de la santé*

Toujours dans le même but de protection de la vie privée, le projet de loi soumet toute communication de données à caractère personnel par ou à la plate-forme eHealth à une autorisation de principe de la section santé du comité sectoriel de la sécurité sociale et de la santé. Ce comité vérifiera si l'échange de pareilles données est "conforme aux dispositions légales et réglementaires relatives à la protection de la vie privée, et en particulier, s'il répond effectivement aux principes de finalité et de proportionnalité". L'exposé des motifs précise qu' « en vertu de ces principes, les données à caractère personnel ne peuvent en effet être échangées que pour des finalités déterminées, explicites et légitimes et elles doivent être adéquates, pertinentes et non excessives par rapport à ces finalités »[234]. Nous examinerons la signification de tous ces termes et principes au cours de l'examen de la loi relative à la protection de la vie privée. Le comité sectoriel devra en outre examiner les mesures de sécurité appliquées lors de l'échange de données à caractère personnel. Quant aux modalités d'autorisation, elles peuvent être déterminées par arrêté royal.

La loi prévoit cependant des cas dans lesquels pareille autorisation du comité sectoriel ne sera pas requise, le premier concernant les situations dans lesquelles la compétence d'accorder une autorisation est déjà attribuée à la section sécurité sociale de

[234] Exposé des motifs, art. 132.

ce comité ou à un autre comité sectoriel de la CPVP, en vertu d'une disposition légale ou réglementaire; et ce dans le but de ne pas porter atteinte aux compétences et missions existantes des divers comités sectoriels. L'exposé des motifs cite à titre d'exemple, l'article 15, § 2, 1°, de la loi du 15 janvier 1990 relative à la BCSS. En vertu de cette disposition, c'est la section sécurité sociale qui est compétente pour accorder une autorisation pour la communication de données à caractère personnel relatives à la santé par une institution de sécurité sociale à une autre institution de sécurité sociale pour l'accomplissement des tâches qui lui sont légalement confiées. Remarquons que cette disposition risque d'être fréquemment d'application, 'étant donné que la plate-forme eHealth est considérée comme une institution de sécurité sociale, et qu'elle vise à échanger des données principalement avec d'autres institutions de sécurité sociale, telles que les organismes assureurs, l'INAMI, le Fonds des accidents du travail, etc.

Une seconde exception à l'obligation d'autorisation de la section santé du comité sectoriel de la sécurité sociale et de la santé, concerne les communications de données autorisées ou exemptées d'une autorisation de principe conformément à une disposition légale ou réglementaire. Un exemple peut être trouvé dans l'article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, qui exempte d'autorisation de principe la communication effectuée entre des professionnels de santé qui sont tenus au secret professionnel et qui sont associés en personne à l'exécution des actes de diagnostic, de prévention ou de prestation de soins à l'égard du patient. Ainsi, et même si un tel échange s'effectue à l'intervention de la plate-forme eHealth, il ne devra pas faire l'objet d'une autorisation.

En outre, la possibilité est offerte au Roi d'exempter certaines communications d'une autorisation de principe, par arrêté délibéré en Conseil des ministres et après avis de la CPVP (art. 11, 3°).

Enfin, la communication de données à caractère personnel codées effectuée par la plate-forme eHealth lorsqu'elle agit en tant qu'organisme intermédiaire – c'est-à-dire dans le cadre de la mission visée à l'article 5, 8° – à l'attention des ministres et des services publics fédéraux compétents en matière de santé publique ou de sécurité sociale, des Chambres législatives, des institutions publiques de sécurité sociale, de l'INAMI, du KCE et des mutualités dans le cadre de leurs missions légales. Il en résulte que ces destinataires peuvent disposer, sans autorisation d'un comité sectoriel, de données à caractère personnel codées – qu'ils ne sont pas en mesure de mettre en rapport avec les personnes auxquelles elles ont trait – en vue de la réalisation de recherches à l'appui de la politique[235]. L'on pourrait toutefois se demander pourquoi l'ISP demeure exclu de l'énumération de ces destinataires que l'on pourrait qualifier de privilégiés, tout comme c'est le cas de l'INS, ou encore des universités.

5. *Obligation de communication de certaines données*

L'article 12 offre au Roi la possibilité d'obliger les institutions publiques – c'est-à-dire tous les pouvoirs administratifs (services publics, institutions publiques, etc.) tous niveaux de pouvoir confondus – à communiquer de façon électronique à la plate-forme eHealth certaines données dont ils assurent la gestion, de sorte que la plate-forme puisse les transmettre à d'autres destinataires qui en ont besoin pour la réalisation de leurs

[235] Exposé des motifs, art. 132 *in fine*.

tâches. L'exposé des motifs justifie cette disposition par la volonté d'éviter la collecte multiple des mêmes données à caractère personnel par différents acteurs des soins de santé. En effet, puisqu'eHealth n'enregistrera pas elle-même de données, les acteurs des soins de santé conservant leurs tâches en matière d'enregistrement de données, il est estimé utile "de permettre que des données qui sont gérées par une institution publique soient mises, de façon efficace et sécurisée, à la disposition d'autres instances qui ont besoin des données en question pour l'accomplissement de leurs missions"[236]. Une application de cette disposition pourrait, selon l'exposé des motifs, être le cas des données du cadastre des prestataires de soins auprès du SPF Santé publique, qui contient des informations relatives aux diplômes et aux spécialités des prestataires de soins. Une autre illustration est fournie par les données de l'INAMI contenant des informations sur les reconnaissances accordées par cette institution aux prestataires de soins.

L'inverse est possible aussi: le Roi peut obliger la plate-forme eHealth à mettre certaines données à disposition de certaines institutions publiques pour l'exécution de leurs missions respectives. Dans un cas comme dans l'autre, le Comité de gestion de la plate-forme doit être consulté avant l'adoption de l'arrêté royal, ce qui garantit, compte tenue de la composition de ce comité et selon l'exposé des motifs, "une répartition des tâches optimale en matière d'enregistrement et de mise à disposition de données à caractère personnel en fonction des missions des diverses institutions publiques concernées". Il est en outre précisé que cette disposition ne vise qu'à déterminer clairement les responsabilités de chaque institution en matière de conservation et de mise à jour de données authentiques, sans pour autant aboutir à une entrave au bon fonctionnement de soins de santé qui serait perturbé par une interdiction d'enregistrement de certaines données, au nom du fait que la tâche a été confiée à une autre institution[237].

6. Valeur probante des données communiquées par voie électronique

Le projet de loi précise, en son article 13, que "les données communiquées par voie électronique à l'intervention de la plate-forme eHealth, ainsi que leur reproduction sur un support lisible bénéficient, jusqu'à preuve du contraire de la même valeur probante que si elles avaient été communiquées sur support papier". Cela signifie qu'elles présentent un degré suffisant de crédibilité pour être prises en considération comme moyens de preuve[238].

Notons que la version de l'avant-projet de loi reconnaissait une force probante supérieure aux données échangées via la plate-forme eHealth, leur attribuant une présomption d'exactitude. La CPVP s'est prononcée contre cette option, son avis ayant été respecté et l'article 13 ayant été modifié en ce sens.

[236] Exposé des motifs, art. 133.
[237] Exposé des motifs, art. 133.
[238] Exposé des motifs, art. 134.

E. La gestion de la plate-forme eHealth

L'article 15 confie la gestion de la plate-forme eHealth à un Comité de gestion, composé de 30 membres dont un président nommé par le Roi pour une durée de 6 ans. Parmi ses membres figurent des représentants de diverses parties concernées par les soins de santé et la sécurité sociale, à savoir les mutualités, les prestataires de soins, les établissements de soins, le SPF Santé publique, le SPF Sécurité sociale, l'INAMI, le KCE, et l'Agence fédérale des médicaments et des produits de santé. Ces membres ont voix délibérative pour toutes les matières. S'ajoutent à cela d'autres membres ne jouissant d'une voix délibérative que pour certaines matières – définition de la vision, de la mission et du plan stratégique d'eHealth – et voix consultative dans les autres matières. Il s'agit de membres nommés et révoqués par divers ministres, à savoir les Ministres de la Santé publique, des Affaires sociales, de l'Informatisation de l'Etat et du Budget. Enfin, une troisième catégorie de membres n'a que voix consultative, et représente les partenaires sociaux faisant partie du Comité de gestion de la BCSS, l'Ordre des médecins et l'Ordre des pharmaciens.

S'agissant du fonctionnement de ce Comité, le projet de loi prévoit le mode de nomination et de révocation des différents membres, ainsi que la durée de leur mandat. Il dispose également que le Comité de gestion établit son règlement d'intérieur, et que le Roi déterminera le statut administratif et pécuniaire du président, tout comme il lui reviendra d'établir les indemnités et le jeton de présence des membres du Comité de gestion.

Quant aux compétences attribuées au Comité de gestion, elles sont décrites de manière relativement large à l'article 15, § 4. Cet organe sera compétent pour accomplir tous les actes d'administration et de disposition nécessaires à la gestion de la plate-forme eHealth. Il peut pour cela faire appel à la collaboration de tiers.

La gestion journalière de la plate-forme eHealth est attribuée à l'administrateur général de la BCSS, à savoir F. Robben, les compétences relevant de la gestion journalière étant semblables à celles dont sont investies les personnes chargées de la gestion journalière dans les institutions publiques de sécurité sociale. Il s'agit entre autres de la direction du personnel, d'assurer le fonctionnement de l'organisme, de le représenter dans les actes judiciaires et extra-judiciaires et d'agir valablement en son nom et pour son compte, sans avoir à justifier d'une décision du Comité de gestion. Nombreux sont ceux qui contestent le regroupement de diverses compétences dans les mains d'une seule personne, ainsi que nous le verrons ci-dessous. L'exposé des motifs justifie son point de vue en ces termes: "en confiant la gestion journalière à l'administrateur général de la BCSS, il est possible de garantir une politique cohérente, notamment en matière de technologies de l'information et de la communication, tant au sein de la sécurité sociale qu'au sein des soins de santé. Par ailleurs, de services partagés peuvent être envisagés"[239]. C'est donc dans un but d'uniformité et d'économie d'échelle que de tels liens sont créés entre la BCSS et eHealth. L'article 18 énonce, dans le même ordre d'idées, que les services, le personnel, l'équipement et les installations de la BCSS nécessaires au fonctionnement de la plate-forme eHealth sont mises à sa disposition.

[239] Exposé des motifs, art. 136.

L'exposé des motifs justifie cette option en ces termes: "Au cours des 17 dernières années, la BCSS a assuré, dans le secteur de la sécurité sociale qui est plus ou moins apparenté au secteur des soins de santé, une fonction comparable à celle qu'assurera la plate-forme eHealth dans le secteur des soins de santé. Le lien entre la BCSS et la plate-forme eHealth permet de réutiliser le know-how et les services développés par cette institution. Ceci permet de maximaliser les chances d'un fonctionnement de qualité de la plate-forme eHealth (…) [laquelle] pourra être développée à moindre coût et plus rapidement. Le secteur des soins de santé pourra profiter de la confiance dont jouit la BCSS dans la sécurité sociale en tant que coordinateur de processus d'échange de données électronique sécurisé, sans centralisation inutile et dans le respect des tâches et compétences de chacun"[240].

Le contrôle de la plate-forme eHealth est exercé, en vertu de l'article 16, par les commissaires du gouvernement et les réviseurs qui exercent le contrôle de la BCSS. Quant à l'article 17, il énonce certaines règles en matière d'impôts, qu'il nous semble peu pertinent d'examiner en détail ici, tout comme c'est le cas pour les règles relatives au financement de la plate-forme, ainsi qu'à son personnel.

F. Le Comité de concertation des utilisateurs de la plate-forme eHealth

Le projet de loi crée, en son article 22, un Comité de concertation des utilisateurs destiné à assister le Comité de gestion dans l'accomplissement de ses missions. Il est chargé à cet effet, de proposer des initiatives visant à promouvoir et à consolider la prestation de services électroniques aux acteurs des soins de santé ainsi que toutes mesures pouvant contribuer à un traitement sécurisé et confidentiel des données à caractère personnel relatives à la santé ou à une simplification administrative pour les acteurs des soins de santé. Des groupes de travail peuvent être créés au sien de ce Comité de concertation, qui établit son règlement d'ordre intérieur (art. 22, al. 2). Par contre, c'est le Roi qui décidera de sa composition, qui nommera le président et qui déterminera ses attributions ainsi que ses modalités de fonctionnement (art. 23).

Le but de ce Comité de concertation est vraisemblablement d'associer tous les acteurs des soins de santé à la plate-forme eHealth, et de constituer un espace de dialogue afin de les impliquer dans le développement du projet. En effet, selon l'exposé des motifs, "le comité de concertation doit constituer le forum où se préparent, en concertation avec toutes les parties concernées (prestataires de soins, mutualités, …), l'organisation concrète et le développement de la plate-forme eHealth et où il est recherché une solution pour tous les problèmes y liés". De plus, "la tâche de cet organe au sein de la plate-forme eHealth s'inscrit donc dans un dynamisme de collaboration et dans une initiative de toutes les parties concernées par le fonctionnement de la plate-forme eHealth, y compris les Régions et Communautés. Il se justifie de faire participer les utilisateurs, chacun avec son expérience propre, à l'examen critique et à l'amélioration du fonctionnement concret de la plate-forme eHealth"[241]. La volonté est donc clairement exprimée d'associer tous les acteurs des soins de santé à ce projet. Le texte rappelle toutefois que le pouvoir final de décision appartient au Comité de gestion.

[240] Exposé des motifs, art. 140.
[241] Exposé des motifs, art. 145.

G. L'autorisation d'association

L'article 34 du projet de loi autorise l'Etat – plus précisément le SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement – et l'INAMI à fonder, en collaboration avec les mutualités et les associations de prestataires de soins et d'institutions de soins, une ASBL permettant d'appuyer la promotion de la qualité de la pratique médicale et des instances chargées de cette mission par l'échange de données cliniques. L'article prévoit trois missions pouvant être confiées à cette association, la première consistant en l'organisation des flux de données électroniques pour la collecte, le traitement et la mise à disposition de données cliniques relatives aux prestations remboursables par l'assurance obligatoire soins de santé et indemnités; ainsi que la tâche de confier l'organisation opérationnelle de ces flux de données à un ou plusieurs de ses membres ou à la plate-forme eHealth (art. 34, al. 3, 1°). L'ASBL peut également être chargée de déterminer l'organisation de registres relatifs à différents domaines cliniques et de confier l'organisation opérationnelle de ces registres à un ou plusieurs de ces membres ou à la plate-forme eHealth (art. 34, al. 3, 2°). Enfin, une troisième mission possible chargerait l'ASBL de recueillir des données anonymes et codées, et de les mettre à la disposition du KCE et d'institutions ou d'associations scientifiques en vue de la réalisation d'études scientifiques (art. 34, al. 3, 4°). L'exposé des motifs précise que l'association publie les flux de données et les registres mentionnés sur son site web.

Cette association est "censée être un organe décisionnel dans les domaines précités, au sein duquel toutes les parties intéressées sont représentées"[242]. Cette disposition manifeste une fois de plus la volonté d'associer tous les acteurs concernés par la plate-forme eHealth. L'exposé des motifs explique la mission de cette ASBL de la sorte: il s'agit "de se mettre d'accord avec les partenaires concernés sur la gestion concrète de certains flux de données, qu'ils soient obligatoires ou non. (…) L'objectif est de réaliser une structure générique et souple qui puisse fonctionner dans divers contextes. Les accords qui pourront être fixés au sein de l'ASBL portent notamment sur la détermination des modalités, la définition des flux de données et la fixation des droits d'accès"[243].

L'exposé des motifs énonce que par l'implication des acteurs des soins de santé dans l'organisation des flux de données, une transparence complète peut être créée en ce qui concerne la nature et les finalités de ces flux. En outre, la formule d'une ASBL garantit le caractère non commercial de l'organisation des flux de données, et elle permet à des tiers d'y adhérer de manière flexible De plus, "cette ASBL n'a bien sûr pas pour mission de procéder à une analyse des données ou de se prononcer sur la qualité des soins. L'ASBL concernée ne porte dès lors en rien préjudice aux compétences des organes existants mais comble un vide afin d'organiser des flux de données spécifiques dans le secteur des soins de santé, de manière transparente, sécurisée et non commerciale"[244].

Ces arguments en faveur de la création de cette ASBL visent à répondre à l'objection soulevée par le Conseil d'Etat, selon lequel le recours à la forme juridique d'une ASBL n'est pas sans prêter à la critique. Nous examinerons la position du Conseil

[242] Exposé des motifs, art. 157.
[243] Exposé des motifs, art. 157.
[244] Exposé des motifs, introduction.

d'Etat au cours du paragraphe suivant de cette section. Notons simplement qu' « afin de rencontrer les préoccupations du Conseil d'Etat, il est proposé de prévoir explicitement dans le projet que les statuts de l'ASBL seront soumis à l'approbation des Ministres compétents pour les affaires sociales et la santé publique », tout comme « les comptes annuels seront soumis à l'approbation du Ministre du budget »[245].

Suite à la suggestion de la CPVP, l'alinéa 4 de l'article 34 précise que les missions de l'association ne préjudicient pas aux compétences du Comité sectoriel de la sécurité sociale et de la santé en ce qui concerne l'octroi d'autorisations pour les communications de données à caractère personnel relatives à la santé. Par ailleurs, l'ASBL ne dispose pas d'un système d'information propre (art. 35).

§ 3. – Les recommandations de la Commission de la protection de la vie privée (CPVP) et du Conseil d'Etat

Ainsi que le veut la procédure, divers organes doivent être consultés avant qu'un projet de loi ne puisse être déposé devant les Chambres législatives. C'est ainsi que l'avant projet de loi a fait l'objet d'un examen et d'une évaluation tant par la CPVP que par le Conseil d'Etat.

A. L'avis de la Commission de la protection de la vie privée

Le 2 avril 2008, la CPVP a rendu un avis concernant le projet de loi portant institution et organisation de la plate-forme eHealth[246], se prononçant dans l'ensemble en faveur du projet tout en émettant certaines remarques, objections et suggestions. Nous ne reprendrons ici que quelques points nous paraissant significatifs, sans détailler l'avis dans son ensemble.

La CPVP souligne tout d'abord les mérites du système décentralisé préconisé par la plate-forme eHealth. En effet, "la Commission constate que le présent projet opte pour le stockage décentralisé de données médicales électroniques. Dans un tel système, la structure documentaire existant chez les différents prestataires de soins de santé reste inchangée et chaque prestataire ou établissement de soins de santé reste également entièrement responsable (de la partie) du dossier médical qu'il a créé(e). Dans le contexte de l'échange électronique de données de santé, ce modèle est avancé par le Groupe 29 comme l'un des systèmes recommandés"[247].

Ainsi que nous l'avons signalé au cours de l'examen du contenu du projet de loi, la Commission a souligné l'importance de la confiance que doivent avoir les usagers en eHealth, et a donc insisté pour que le projet de loi reprenne une disposition qui stipule que le projet ne porte en rien préjudice à la loi du 8 décembre 1992 relative à la

[245] Exposé des motifs, art. 157.
[246] Avis de la Commission de la protection de la vie privée n° 14/2008 du 2 avril 2008, à la demande de la Ministre des Affaires sociales et de la Santé publique et de la Ministre de la Fonction publique et des Entreprises publiques concernant un projet de loi portant institution et organisation de la plate-forme eHealth (A/2008/016), http://www.privacycommission.be/fr/docs/Commission/2008/avis_14_2008.pdf.
[247] Avis 14/2008, p. 6, n° 17.

protection de la vie privée à l'égard des traitements de données à caractère personnel, à la loi du 22 août 2002 relative aux droits du patient, ni aux règles légales concernant l'exercice des professions des soins de santé[248]. Cette suggestion a été suivie et une disposition a été insérée dans le projet de loi en ce sens (art. 6).

Un autre aspect positif retenu par la CPVP tient au respect, par la plate-forme eHealth telle qu'établie par le projet de loi, des principes de loyauté, licéité et finalité, de proportionnalité, de précision et exactitude, de transparence, et de sécurité[249]. De plus, la CPVP remarque que le répertoire de référence n'est pas une banque de données à caractère personnel contenant des données à caractère personnel de contenu: il contient uniquement des références, par patient – exclusivement les patients qui y consentent –, relatives aux acteurs de soins de santé qui conservent un dossier concernant ce patient.

La CPVP opère un important revirement de jurisprudence au sujet de l'utilisation du numéro du Registre national, qu'elle justifie de la sorte:

"Il existe plusieurs méthodes pour parvenir à une protection efficace et performante de la vie privée. Grosso modo, on connaît d'une part les méthodes légales (législation et réglementation qui sont imposées par les instruments de droit) et d'autre part, les possibilités techniques (barrières matérielles et technologiques). Un système de protection aura normalement recours à ces deux modes.

45. La question se pose de savoir dans quelle mesure il est ou non utile ou nécessaire d'utiliser une identification sectorielle spécifique (plutôt qu'une identification générale comme le numéro d'identification de la sécurité sociale) lors du traitement de données à caractère personnel relatives à la santé. Une identification sectorielle spécifique consisterait alors en un code ou en un numéro qui serait déduit du numéro d'identification de la sécurité sociale et qui pourrait ou devrait uniquement être utilisé pour certains traitements ou certaines finalités. Cette identification spécifique serait alors le code spécifique pour le secteur "soins de santé", limité ou non aux traitements dans le cadre des prestations curatives, strictement médicales ou élargies à l'ensemble des traitements sur le plan médical et paramédical, ou dans le domaine de la prévention, des mutualités, des obligations de droit social, de l'administration, etc.

46. Il est évident que le choix d'un identifiant sectoriel n'est utile que lorsque les instances qui doivent s'échanger des données à caractère personnel recourent à un même identifiant lors de ces échanges et donc, qu'un même algorithme est utilisé par tous pour déduire l'identifiant sectoriel du numéro d'identification de la sécurité sociale. La définition d'un tel algorithme pourrait être assumée par la plate-forme eHealth en tant qu'élément de son ensemble de tâches. Cette spécialisation de l'identifiant pourrait en outre encore être ventilée par exemple selon le type de prestataire de soins (un médecin généraliste, un hôpital, un laboratoire, une mutualité qui attribue un numéro unique par patient). On peut encore aller plus loin en codant de manière unique chaque prestation et chaque acte médical. Techniquement, tout cela est possible.

47. Il va de soi que la limitation de l'utilisation d'identifiants spécifiques à des secteurs d'application aussi restreints que possible peut rendre le "couplage" de données à caractère personnel plus difficile en dehors de ces secteurs d'application.

48. Il est toutefois tout aussi évident qu'un tel codage doit toujours être suivi d'un déchiffrage ou décodage. Il s'agit en effet (presque) toujours d'un genre de "chaîne"

[248] Avis 14/2008, pp. 7-8, n° 21-22.
[249] Avis 14/2008, pp. 8-9.

d'informations qui doivent être couplées les unes aux autres pour parvenir à certaines représentations, poser des actes, administrer une médication ou des soins, assurer le suivi et tenir à jour le dossier de suivi administratif. Un problème supplémentaire se pose à cet égard : il peut en effet également arriver que l'on doive pouvoir détecter non seulement la personne, mais aussi parfois certains éléments matériels comme des médicaments ou des prothèses, des implants, etc. Se pose en outre la problématique de la recherche scientifique.

49. Le décodage doit donc pouvoir se faire de manière rapide et sans erreur, et ce sans générer la moindre charge administrative. Dans cette optique, n'appliquer aucun codage (ni décodage) assurerait la plus grande certitude.

50. Le fait de travailler avec une clé d'identification unique constitue le "degré zéro" du codage : le numéro d'identification de la sécurité sociale a justement pour but d'éviter le moindre doute quant à l'identification précise d'une personne. Si notre "nom" était unique, il suffirait en tant qu'identifiant unique. Ce n'est pas le cas (et un numéro standardisé est également plus facile à utiliser dans les TIC).

3.4.3. Analyse et avis de la Commission.

51. Jusqu'à présent, la Commission a déjà souligné à plusieurs reprises la nécessité d'élaborer des numéros d'identification spécifiques à un secteur déterminé. À cet égard, elle a toujours attiré l'attention sur les dangers éventuels – notamment les couplages effrénés de données à caractère personnel – liés à un numéro d'identification qui est utilisé dans plusieurs secteurs. La Commission rappelle son inquiétude à ce sujet.

52. La Commission prend acte du fait que – contrairement à ce qui se fait dans d'autres États membres de l'Union européenne –, il n'y a pas d'enregistrement central de données dans la plate-forme eHealth. En prenant pour exemple la Banque-carrefour de la sécurité sociale, on a prévu la création d'un répertoire des références qui doit permettre d'afficher à l'écran les données nécessaires par patient et ce, au moyen d'une connexion temporaire avec la base de données où sont enregistrées ces données spécifiques.

53. Un tel système ne permet pas en soi de traiter des données en créant des catégories sur la base du fait que la situation médicale de certaines personnes présente des caractéristiques communes, de rassembler toutes les données de santé relatives à une seule personne, ni d'effectuer des couplages non autorisés de données de santé avec d'autres données à caractère personnel (données sociales, fiscales, familiales, ...).

54. Comme mentionné ci-dessus, le projet opte de facto pour l'utilisation d'une clé d'identification unique générale : le numéro d'identification de la sécurité sociale, le cas échéant le numéro de Registre national.

55. Cette option est également fermement motivée dans l'exposé des motifs du projet : "L'utilisation d'une clé d'identification unique offre des garanties pour une identification correcte des intéressés à chaque stade de l'échange de données à caractère personnel, c'est-à-dire tant pour l'émetteur que pour le destinataire des données à caractère personnel et pour les éventuels autres intervenants."

56. Un numéro d'identification spécifique pour les soins de santé ne sera, de par ce choix, pas appliqué en ce qui concerne l'échange de données à caractère personnel via la plate-forme eHealth.

57. Dans le prolongement de la jurisprudence citée, la Commission a examiné la question de savoir si l'utilisation du numéro d'identification du Registre national ou du

numéro d'identification de la sécurité sociale comme identifiant unique au sein de la plate-forme eHealth était recommandée.
58. Vu qu'une identification correcte est d'une importance primordiale d'une part, et qu'au stade actuel des choses, il n'y a pas d'argument suffisant qui s'y oppose d'autre part, il est recommandé de soutenir l'option d'un identifiant fort tel que le numéro d'identification de la sécurité sociale.
59. Un numéro de santé sectoriel général serait utilisé par un nombre si élevé de personnes qu'il n'offrirait peut-être pas une meilleure protection efficace et perceptible de la vie privée. L'utilisation d'un tel numéro sectoriel risque également de devenir une charge organisationnelle importante pour la plate-forme eHealth, ce qui pourrait donner lieu à une identification inefficace.
60. De plus, le développement d'un numéro de santé sectoriel occasionnerait également des problèmes spécifiques. Les méthodes qui entrent en ligne de compte pour l'élaboration d'un tel numéro présentent en effet d'importants inconvénients.
61. Les systèmes suivants sont envisageables en théorie : soit chaque acteur (médecin, hôpital, laboratoire médical, ...) attribue à ses patients un numéro propre (ce qui implique donc qu'un patient recevrait plusieurs numéros), soit chaque patient reçoit un seul numéro de santé et ce, au moyen d'un algorithme appliqué au numéro d'identification de la sécurité sociale. Les défauts de ces méthodes sont expliqués ci-après.
62. Dans l'hypothèse où un patient recevrait plusieurs numéros spécifiques (chez son médecin traitant, à l'hôpital, ...), il faudrait mettre au point des méthodes permettant aux systèmes informatiques des divers acteurs de toujours pouvoir identifier correctement le patient sur la base de ces différents numéros.

Pour ce faire, deux solutions sont possibles :

- soit un logiciel spécial, conçu par eHealth et chargé des conversions nécessaires, est installé chez chaque acteur. Ceci impliquerait évidemment un défi organisationnel difficilement réalisable ;

- soit les conversions sont effectuées par la plate-forme eHealth, ce qui conduirait inévitablement à la constitution d'un monopole au profit de cette instance – ce qui n'est pas souhaité par le projet de loi.

63. L'hypothèse où chaque patient recevrait un seul numéro d'identification, spécifique au secteur de la santé mais utilisé par chacun au sein de ce secteur et créé par l'application d'un algorithme au numéro d'identification de la sécurité sociale, implique que cet algorithme doive être utilisé par tous les établissements de soins et tous les prestataires de soins. La Commission est consciente du fait qu'en pareil cas, la déduction du numéro d'identification spécifique au secteur de la santé est généralement possible et que l'utilisation d'un tel numéro spécifique offre à peine une protection supérieure contre un couplage illégitime de données à caractère personnel. Cette protection supplémentaire minimale ne compense donc pas le coût plus élevé et le risque d'erreurs lors de l'échange de données à caractère personnel lorsque celui-ci est permis.

64. La Commission conclut que compte tenu de tous les facteurs susmentionnés, l'instauration d'un numéro de santé sectoriel n'est pas l'instrument le plus recommandé pour garantir la protection de la vie privée. Selon la Commission, l'application d'autres techniques de protection de la vie privée, comme la création d'un système dans lequel les données ne font pas l'objet d'un enregistrement centralisé et l'exigence d'une autorisation par le comité sectoriel en combinaison avec la désignation d'un médecin contrôleur et d'un conseiller en sécurité de l'information, doit suffire pour pouvoir empêcher des couplages non souhaités et interdits de différents fichiers de données via la plate-forme eHealth.
65. La Commission émet donc un avis favorable pour l'utilisation du numéro de Registre national et l'accès aux données qui sont demandés"[250].

S'agissant de la mission exercée par eHealth en tant qu'organisation intermédiaire, visée à l'article 1, 6° de l'A.R. du 13 février 2001, la CPVP ne soulève pas d'objection majeure, se contentant d'insister sur la nécessité de ne conserver que les données à caractère personnel nécessaires aux traitements ultérieurs à des fins historiques, statistiques ou scientifiques, sous une forme qui permette l'identification de la personne concernée mais qui ne communique pas par elle-même les données à caractère personnel de celle-ci.[251]. Cette garantie a été inscrite dans le projet de loi, l'avis de la CPVP ayant été pris en compte à ce sujet.

Enfin, la CPVP refuse qu'une présomption d'exactitude soit attribuée aux données échangées via la plate-forme eHealth, préférant leur reconnaitre la même force probante que les données échangées par support papier[252]. Sur ce point également, son avis a été respecté et le projet de loi adapté en conséquence.

B. L'avis du Conseil d'Etat

Le Conseil d'Etat a lui aussi été saisi d'une demande d'avis sur l'avant projet de loi portant institution et organisation de la plate-forme eHealth. Après avoir examiné l'affaire au cours des séances du 17 et du 21 avril 2008, il a rendu un avis lui aussi favorable dans l'ensemble, tout en se montrant plus critique sur certains points[253].

En effet, le Conseil d'Etat commence par soulever une contradiction existant entre la création d'une "institution publique dotée de la personnalité juridique" mais "au sein de la BCSS". Selon l'organe, certaines dispositions laissent à penser qu'eHealth est intégrée à la BCSS – comme par exemple les dispositions relatives au contrôle administratif, à la mise à disposition du personnel et de l'équipement de la BCSS, au rôle de l'administrateur général de la BCSS, etc. –, tandis que d'autres laissent à penser qu'il s'agit d'une institution distincte. Il recommande alors de définir précisément le statut juridique de la plate-forme eHealth, ainsi que les rapports qu'elle entretient avec la BCSS. L'exposé des

[250] Avis 14/2008, pp. 13-17, n° 44 à 65.
[251] Avis 14/2008, p. 17, n° 66 et s.
[252] Avis 14/2008, p. 22, n° 93-95.
[253] Avis du Conseil d'Etat n° 44.351/1/2/3/4, joint au projet de loi portant dispositions diverses (I), déposé à la Chambre des Représentants le 29 mai 2008, Doc. 52 1200/001, http://www.lachambre.be/FLWB/PDF/52/1200/52K1200001.pdf.

motifs répond partiellement à cette remarque, en précisant qu'eHealth est à considérer comme une institution publique de sécurité sociale. Quant aux rapports qu'elle entretient avec la BCSS, il nous semble que le projet de loi demeure relativement vague à ce sujet, manquant de la sorte de répondre au souhait de précision du Conseil d'Etat.

En outre, le Conseil d'Etat critique le recours à la technique de droit privé de l'ASBL pour la gestion des flux de données, et ce pour diverses raisons. Tout d'abord, "l'accomplissement des tâches de l'association – qui concernent en partie des missions de l'autorité – et l'utilisation des fonds publics pour financer l'association sont en grande partie soustraits au contrôle parlementaire direct". En outre "prévaut le principe que les compétences confiées à une association sans but lucratif ne peuvent concerner des missions essentielles de l'autorité et que l'autorité ne peut se départir de ses compétences, sans restrictions et d'une manière générale, notamment dans la mesure où ces compétences impliquent des choix politiques". Ces arguments ont d'autant plus d'importance que l'ASBL intervient dans le traitement de données médicales à caractère personnel. Le Conseil d'Etat recommande alors de vérifier si la forme d'une ASBL est vraiment nécessaire, et si la forme d'un organisme public ne pourrait suffire. Dans l'exposé des motifs, le gouvernement répond à cette critique de la sorte: "Avec la création de l'ASBL en question le gouvernement souhaite créer, par analogie avec le registre du cancer, un accord de coopération dans le cadre duquel des acteurs publics et privés peuvent prendre des décisions communes, de façon organisée et structurée, en ce qui concerne la collecte, le traitement et la mise à disposition de certaines données cliniques. Il convient de souligner qu'il n'est pas question en l'occurrence d'un transfert de compétences des autorités vers une personne morale de droit privé. L'ASBL en question ne disposera d'aucun pouvoir réglementaire pour imposer ou rendre obligatoire certaines collectes ou certains traitements de données. Il n'est donc pas porté atteinte aux compétences légales établies dans le cadre de l'assurance soins de santé et indemnités"[254]. Rappelons qu'une disposition a été insérée dans le projet de loi afin de rencontrer les préoccupations du Conseil d'Etat à ce sujet, soumettant les statuts de l'ASBL ainsi que ses comptes annuels à l'approbation des ministres compétents (art. 34, al. 5).

Le Conseil d'Etat a par ailleurs formulé la même remarque que la CPVP en ce qui concerne la force probante des données échangées via la plate-forme eHealth. Il a en outre dénoncé l'imprécision du critère déterminant les membres ayant voix délibérative – ce critère étant formulé en termes de "définition de la vision et de la stratégie" –, comme étant trop vague pour être efficace. Aucune modification n'a toutefois été apportée au projet de loi sur ce point.

Enfin, la délégation au Roi prévue à l'article 30 est, selon le Conseil d'Etat, trop vague et non justifiée. Il s'agit de la possibilité « d'abroger, compléter, modifier ou remplacer les dispositions légales applicables afin de permettre à la plate forme eHealth de réaliser son objectif et de remplir ses missions ». Cette disposition vise les processus impliquant un échange de données à caractère personnel sur support papier, dont l'abrogation est nécessaire pour permettre de réaliser dorénavant cet échange par voie électronique à l'intervention de la plate-forme eHealth[255]. Le Conseil d'Etat recommande de circonscrire plus clairement l'objet de cette délégation, et de démontrer que le législateur se trouve dans l'impossibilité de prendre lui-même cette mesure, parce que la

[254] Exposé des motifs, art. 157.
[255] Exposé des motifs, art. 153.

durée de la procédure parlementaire ne permettrait pas de réaliser avec la promptitude voulue l'objectif d'intérêt général visé. Il n'est toutefois pas certain, selon le Conseil d'Etat, que ce soit le cas en l'occurrence, mais si les auteurs du projet estiment le contraire, ils doivent le justifier dans l'exposé des motifs. Ce dernier n'y répond que de manière vague, en précisant que "la compétence du Roi en la matière est limitée: les arrêtés royaux en question ne peuvent modifier la portée générale des dispositions et ils doivent être sanctionnés par une loi avant la fin du treizième mois suivant leur entrée en vigueur"[256]. En outre, l'avis de la CPVP sera requis, suite à sa propre proposition.

§ 4. – Les critiques adressées par les associations de médecins

Ainsi que nous l'avons déjà évoqué, le projet eHealth est loin de faire l'unanimité auprès des différents acteurs concernés. Les associations de médecins principalement, mais également divers experts en la matière, critiquent le projet dont certains aspects leur paraissent dangereux, voire intolérables.

A. La réaction de l'Association belge des syndicats médicaux (ABSyM)

Suite au dépôt du projet de loi portant dispositions diverses (I) devant la Chambre des Représentants le 29 mai 2008, l'Absym organisa, le 9 juin 2008, une conférence de presse. L'interview de Roland Lemye, président de l'Absym[257], révèle les critiques adressées au projet par les prestataires de soins de santé, dont voici les principaux aspects.

Plusieurs éléments provoquent une grande inquiétude dans le chef des médecins, qui ne se sentent pas du tout rassurés face à ce projet eHealth. En effet, R. Lemye "estime que le gouvernement, en voulant voter rapidement ce texte dans le cadre d'une série de dispositions réglementaires, fait preuve d'une volonté d'efficacité mais pas de protection de la confidentialité des données médicales"[258]. Tout d'abord, selon le médecin, ce projet s'est développé dans l'opacité, avec une volonté manifeste d'écarter les médecins de la réflexion. Le projet leur a été présenté une fois ficelé, et cette opacité génère des craintes. Ensuite, les finalités du projet exigent une récolte de données, dont il n'est pas question dans le projet. Celui-ci mentionne en effet le fait que les données puissent servir à la politique de soins de santé, ce qui exige une récolte. Mais rien n'est précisé quant aux moyens de réaliser cette récolte: les données seront-elles nominatives, codées, anonymes? Visiblement cela dépendra des cas. Mais ce manque de précision n'offre aucune garantie à ce sujet. Quant à la concentration des pouvoirs entre les mains d'une seule et même personne, R. Lemye précise qu'il n'a rien contre Frank Robben, mais il souligne que celui-ci est administrateur général de la BCSS ainsi que de l'informatique des administrations via la Smals. Pour cette raison, il devrait être séparé d'une banque carrefour des données de santé, en raison du caractère sensible de celles-ci. Or, on lui en

[256] Exposé des motifs, art. 153.
[257] http://fr.medisurf.be/protected/archives/WebTV/Archief/20080610.html.
[258] Journal du Médecin n° 1925 du 10 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1925/9b9ab90e-d0b8-4262-8f11-8a267d972810.vak.html.

propose l'administration! De plus, il est membre de la CPVP, et plus particulièrement de la section santé du comité sectoriel de la sécurité sociale et de la santé. La CPVP est présentée dans le projet comme une protection, mais cela n'a rien de rassurant dès lors que F. Robben en est membre. "Quand il demande une autorisation, c'est un peu comme s'il se la donnait à lui-même"[259].

Suite à l'intervention de l'Absym, quelques modifications ont été apportées au projet de loi, mais de manière bien insignifiante. Par exemple, le nombre des médecins présents au sein du Comité de gestion est passé de un à trois, mais sur un total de trente personnes, ce qui n'offre aucune garantie quant à la prise en considération des préoccupations du corps médical. Parmi ces préoccupations figure celle tenant à la confiance nécessaire à la relation médecin-patient, que les médecins sont soucieux de protéger. Vis-à-vis du patient, le médecin s'engage à être responsable de la confidentialité des données, sinon le patient ne confierait plus rien à son médecin. Le monde politique ne les a pas entendus. Selon Jacques de Toeuf, vice-président de l'Absym, "ce système va donner le libre accès à des données médicales sans que le patient ne le sache. Ces informations vont être accessibles à des gens qui vont vérifier ce que le patient consomme, s'il consomme 'bien' et dans le cadre de ce qui est défini par le budget. C'est redoutable. 10 millions de Belges vont se retrouver sur liste noire de consommateurs de soins". Pour le chirurgien bruxellois, il est clair que, dans un tel contexte, toutes les expériences-pilotes qui reposent sur le partage de données, telles que les trajectoires de soins, ne sont plus à l'ordre du jour. "C'est terminé! Si on permet à des tiers, qui n'ont rien à voir avec la relation thérapeutique, d'avoir accès à ces informations, ce n'est plus possible"[260].

Un autre élément inquiétant tient au fait que le Comité de gestion prend déjà des décisions sans que personne n'y ait été nommé, en tout cas pas les médecins qui doivent en faire partie. De même, l'ASBL eCare, créée pour gérer le flux des données, prend déjà des décisions, agrée des projets, etc., alors qu'elle devrait être créée par la loi. Elle n'a donc encore aucune existence légale. Enfin, la section santé du comité sectoriel de la sécurité sociale et de la santé n'est pas nommée mais il existe déjà une autorisation d'utiliser le numéro du Registre national. "Le Comité sectoriel de la santé aurait changé d'avis en acceptant l'utilisation du numéro de registre national comme identifiant. En principe, cette commission doit être composée de médecins. Ceux-ci n'ont pas encore été nommés. Le comité ne peut donc pas donner d'avis"[261]. Selon les représentants de l'Absym, cela montre qu'aucune garantie n'est offerte quant à l'imperméabilité avec les administrations telles que la justice, etc.

Tout cela démontre qu'e-Health a déjà l'air de fonctionner alors que les médecins n'ont ni été invités à un comité de gestion, ni vu la publication des nominations des membres des comités. "Des fonctionnaires de l'INAMI se présentent déjà comme travaillant pour la structure eCare (structure mère qui accueille la plateforme de transfert de données e-Health). Manifestement, le projet avance sans que nous soyons au courant.

---

[259] Journal du Médecin n° 1925 du 10 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1925/9b9ab90e-d0b8-4262-8f11-8a267d972810.vak.html.

[260] Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html.

[261] Journal du Médecin n° 1925 du 10 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1925/9b9ab90e-d0b8-4262-8f11-8a267d972810.vak.html.

Ce manque de transparence est inquiétant. Quand on ne veut pas être transparent, c'est qu'il y a des choses à cacher"[262].

Pour le Dr Lemye, il est impératif de définir comment les autorisations pour accéder aux dossiers médicaux vont être délivrées. "D'après mes informations, un médecin serait autorisé à consulter les données à partir du moment où il possède un numéro INAMI. Ce critère est tout à fait insuffisant: un médecin agréé par l'INAMI n'a pas le droit de consulter 10 millions de dossiers médicaux. Imaginons que ce médecin soit à la fois médecin traitant et travaille à temps partiel pour une compagnie d'assurances ou pour une banque, il pourrait avoir accès à des données sensibles. C'est inquiétant"[263]. Le médecin ajoute: "L'exposé des motifs précise que 'la plate-forme n'enregistrera pas elle-même des informations de contenu de façon centralisée', mais signale ailleurs que 'elle permettra un meilleur appui de la politique de santé notamment en assurant un suivi longitudinal des patients atteints de différentes pathologies'". Comment un pareil suivi serait-il possible sans enregistrement des données?, s'interroge Roland Lemye, président de l'Absym. De fait, le même document précise que 'la plate-forme peut prêter sa collaboration à des études scientifiques et d'appui à la politique en matière de soins de santé en recueillant les données à caractère personnel utiles auprès des acteurs concernés des soins de santé.' Il précise aussi 'qu'afin d'éviter la collecte multiple des mêmes données à caractère personnel, il peut cependant être utile de permettre que les données qui sont gérées par une institution publique soient mises, de façon efficace et sécurisée, à la disposition d'autres instances qui ont besoin des données en question pour l'accomplissement de leurs missions'. Il est donc possible qu'une fois récoltées, les données puissent être accessibles à différents organismes publics sans que le patient ou le médecin en soient eux-mêmes conscients. L'ambiguïté est en outre continuellement entretenue sur le caractère nominatif, codé ou anonyme des données."[264].

Dans une réaction écrite, R. Lemye souligne l'insuffisance de la garantie tenant à l'autorisation du patient que ses données soient échangées via la plate-forme eHealth. En effet, "le patient est-il bien éclairé? Ne subira-t-il pas les pressions d'un médecin au service d'une assurance, d'une banque, d'un employeur? Il est donc nécessaire que le médecin autorisé précise en quelle qualité il agit par une carte d'identification et que son passage laisse une trace"[265]. Le Dr. Lemye dénonce le fait que "le projet privilégie l'efficacité des échanges, la gestion de l'assurance-maladie, le soutien à la politique des soins de santé, la connaissance des dossiers patients par les mutuelles et pas la confidentialité et la vie privée. Les conséquences en seront que la décision médicale échappera au médecin et sera prise par le monde politique et les mutuelles. Quand le patient s'apercevra, après coup, de la perte de confidentialité, il ne se confiera plus au médecin et la relation thérapeutique souffrira de cette perte de confiance. Le caractère humain des soins de santé, alors, disparaîtra".

Marc Moens, vice-président de l'Absym, s'est quant à lui exprimé devant la Commission de la santé publique de la Chambre des Représentants lors de son audition.

---

[262] Journal du Médecin n° 1925 du 10 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1925/9b9ab90e-d0b8-4262-8f11-8a267d972810.vak.html.
[263] Journal du Médecin n° 1925 du 10 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1925/9b9ab90e-d0b8-4262-8f11-8a267d972810.vak.html.
[264] Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html.

Après avoir dénoncé le secret et la précipitation dans lesquels le projet eHealth a été mené, il déclare l'Absym "convaincue de la nécessité d'un système électronique fonctionnant correctement dans le domaine des données relatives aux soins de santé". Cependant, M. Moens ajoute qu' "il y a deux conditions absolues: la sécurité et la confiance, lesquelles sont du reste étroitement liées. L'Absym est d'avis qu'aucune des deux conditions n'est remplie de manière satisfaisante dans le projet de sorte que celui-ci doit être remanié en profondeur"[266]. Pour le reste, il reprend les critiques de R. Lemye détaillées ci-dessus, au sujet de l'importance de l'indépendance de la plate-forme eHealth vis-à-vis de la BCSS, de l'opacité du cadre légal au niveau du Comité sectoriel de la sécurité sociale et de la santé, et du non respect de la loi créant Be-Health.

De plus, il déclare inacceptable l'intervention d'eHealth en tant qu'organisme intermédiaire, justifiant son point de vue de la sorte: "S'agissant de recueillir, agréger, coder ou anonymiser des données en tant que «*Trusted Third Party*» (TTP), la toute première exigence, selon les règles de l'art, est qu'il faut une «indépendance» tant à l'égard de l'émetteur que du récepteur. Concernant le projet de loi à l'étude, ce n'est le cas ni de manière structurelle, ni lorsque l'on considère les membres dans les comités de gestion de toutes les parties communicantes. Bien au contraire, ceux qui recueillent, qui assument le rôle de TTP, qui agrègent les données, les transmettent et même les traitent ne sont pas indépendants les uns des autres. En outre, cette même structure désigne son propre conseiller en sécurité pour se contrôler soi-même. L'Absym réclame une organisation intermédiaire indépendante qui est chargée, avec les garanties nécessaires, du cryptage des données et de l'éventuelle transmission de ces données à la plate-forme eHealth. La perception du projet est incontestablement que eHealth servira exclusivement à simplifier la vie des Autorités et des Mutuelles et à augmenter leurs possibilités de contrôle"[267].

Enfin, M. Moens dénonce le caractère hypothétique de l'utilisation non-obligatoire de la plate-forme eHealth, avancé publiquement comme une justification par F. Robben. Il estime en effet que "si seul eHealth a le droit d'utiliser le numéro du registre national sans devoir passer par la Commission de la protection de la vie privée, si seules les données communiquées sur la plate-forme eHealth bénéficient de la valeur probante, s'il n'est pas précisé préalablement que les registres et sources authentiques financés avec de l'argent public seront également mis à la disposition de tiers ne souhaitant pas utiliser la plate-forme eHealth et si, pour finir, une gratuité du service est prévue, le «caractère non obligatoire» devient très hypothétique"[268].

---

[266] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 24, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[267] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 26, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[268] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 26-27, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

B. Réaction du Forum des associations de généralistes (FAG)

S'exprimant au nom du Forum des associations de généralistes (FAG) devant la Commission de la Santé publique, Jean-François Souppart dénonce également le manque de concertation du corps médical dans ce projet, en commençant son audition en disant qu'il "craint être invité à jouer dans une pièce où tout est déjà écrit à l'avance"[269]. En effet, si le projet Be-Health "a quitté l'avant-scène médiatique depuis plusieurs années, il n'en a pas moins continué à évoluer dans l'ombre, sans que les prestataires de soins ne soient tenus informés de l'état d'avancement des travaux, des standards de communication choisis ni de l'origine du financement qui a permis la poursuite des travaux".

J.-F. Souppart cite le cas du Réseau Santé Wallon (RSW) et son homologue bruxellois du RSWX, l'ASBL Abrumet, au sein desquels les cercles de médecins généralistes collaborent activement et son largement représentés dans les organes de décision[270], ce qui est loin d'être le cas du projet eHealth. Notons que des représentants de ces divers projets similaires à eHealth ont également été entendus à la Commission de la santé publique, ce qui leur a permis à leur tour de déplorer le manque de concertation des acteurs de terrain, ainsi que le revirement de jurisprudence quant à l'utilisation du numéro d'identification du registre national et non d'un numéro spécifique au secteur de la santé – système utilisé par le RSW[271].

Le représentant du FAG dénonce en outre l'utilisation du numéro du Registre national, la sous-représentation des médecins au sein du Comité de gestion, la concentration des pouvoirs dans les mains de la BCSS, la large délégation de pouvoirs au Roi, ou encore le caractère vague des dispositions traitant de l'ASBL à créer. Il plaide en faveur d'un moratoire, qui devrait être mis à profit pour associer dans la réflexion tous les acteurs de terrain concernés comme les syndicats de médecins, de kinésithérapeutes, d'infi rmiers et d'auxiliaires médicaux, l'Ordre des médecins, les sociétés scientifiques de médecine générale, les réseaux régionaux de télématique médicale (RSW, ABRUMET), la Commission de la protection de la vie privée, l'INAMI et les organismes assureurs"[272].

---

[269] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 27, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[270] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 29, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[271] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 41-49, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[272] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 31, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

C. Réaction du Conseil national de l'Ordre des Médecins[273] (CNOM)

Le CNOM s'étonne qu'un projet de loi de l'ampleur d'eHealth soit traité dans l'urgence, sans concertation avec les intéressés, et dans le cadre d'une loi "fourre-tout". C'est entre autres le principe du secret professionnel du médecin, clé de voûte du système des soins de santé, selon Benoît Dejemeppe (président suppléant du CNOM), qui pose problème. En effet, le projet de loi est susceptible d'avoir d'importantes répercussions sur ce principe, ce qui justifierait un débat approfondi sur la question. En outre, le CNOM n'a pas été informé de l'état d'avancement du projet, malgré ses demandes réitérées.

Une importante critique que le CNOM adresse tient au fait que "la plate-forme e-Health n'est pas qu'un système de transmission de données personnelles concernant les patients. "Elle enregistre des données médicales personnelles, non expressément et préalablement déterminées. Ceci n'est assurément pas sans conséquence sur le respect de la vie privée et le secret professionnel. Ainsi par exemple, le Conseil national constate que le répertoire des références mentionne les acteurs de soins de santé auprès desquels les patients souhaitent ou non que leurs données soient conservées et les modalités de leur accès. Le simple fait de mentionner que le patient consulte tel ou tel praticien peut révéler en soi un diagnostic médical et comporte un risque de stigmatisation. En effet, le seul fait de mentionner qu'un patient consulte un psychiatre ou un spécialiste du sida est une donnée devant être couverte de façon absolue par le secret médical"[274].

Quant à la concentration des pouvoirs dénoncée par l'Absym, le CNOM "refuse et s'oppose de façon absolue à la centralisation par une seule instance des systèmes de sécurité et d'identification, de la gestion des transactions, de la labellisation des logiciels et du transfert des données. "En particulier, la plate-forme e-Health ne peut assurer le rôle d'organisation intermédiaire et gérer de ce fait les clés de codification permettant d'associer les données codées aux patients"[275].

En conclusion, l'Ordre des médecins ne remet pas en cause l'importance du projet, mais demande qu'un débat approfondi soit tenu sur la question.

D. Les critiques adressées quant à la méthode

Nombreux sont ceux qui critiquent la méthode suivie pour l'élaboration du projet eHealth, qu'ils se prononcent en faveur ou à l'encontre de celui-ci. En effet, s'il n'est pas surprenant d'entendre les associations de médecins s'insurger contre le fait qu'ils n'aient

---

[273] Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html; file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/ordre%20des%20m%C3%A9decins.htm.

[274] Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html; file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/ordre%20des%20m%C3%A9decins.htm.

[275] Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html; file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/ordre%20des%20m%C3%A9decins.htm.

pas été consultés ni impliqués dans ce projet, il est en revanche plus étonnant d'entendre les parlementaires eux-mêmes regretter ce manque de concertation des acteurs de terrain, après avoir reconnu leur accord quant aux objectifs de ce projet.

Daniel Bacquelaine fait partie de ceux-ci, déplorant au nom du MR à la Chambre des Représentants le fait que les associations de professionnels n'aient pas été impliquées plus tôt et plus fortement dans la genèse de ce projet. Il recommande de veiller à ce que le cas du projet eHealth et du mécontentement qu'il suscite à cause de ce manque de concertation ne consiste pas en un précédent, estimant qu'en matière de santé publique il est important que les acteurs de terrains s'associent au projet et le considèrent utile à leur pratique. Le médecin ne s'oppose pas au projet, mais précise qu'il convient de favoriser l'utilisation de cette plate-forme, sans quoi elle deviendrait une coquille vide, puisque l'utilisation d'eHealth est facultative. Il faut donc recréer une confiance suffisante des prestataires de soins et des professionnels de la santé en ce système, et leur offrir les garanties qu'ils attendent. Il convient également de favoriser une concertation et de lever un certain nombre d'incertitudes au cours des débats qui auront lieu au Sénat, ainsi que lors de l'élaboration des arrêtés d'exécution de la loi[276].

Dans le même ordre d'idées, Georges Gilniket s'insurge, au nom du parti Ecolo-Groen, contre la méthode de travail qu'il dénonce comme étant "peu à l'écoute des acteurs de terrain". Il reproche à la Ministre Onkelinx d'avoir créé une opposition massive plutôt que d'avoir convaincu les acteurs de terrain, et d'ainsi avoir "réussi l'exploit de rassembler toutes les associations médicales contre ce projet, de l'Absym aux maisons médicales! Leur avis, particulièrement dur, résulte d'une absence de concertation préalable et dénote un malaise. Comment imaginer une mise en œuvre sans la participation de ces acteurs?". Lorsque la ministre lui répond que des auditions ont été organisées à ce sujet, il rétorque que celles-ci se sont déroulées en trois jours, de manière tellement précipitée que les experts écoutés découvraient le texte[277].

Au Sénat, le rapporteur de la Commission des affaires sociales a également regretté et dénoncé de manque de concertation avec les acteurs du terrain. Il ajoute qu'"une meilleure concertation préalable et une discussion approfondie avec les futurs acteurs du système auraient permis à tout le moins de préciser plusieurs points essentiels", parmi lesquels il cite le consentement du patient, qui selon lui doit être libre, spécifique et éclairé quant à la finalité de l'utilisation de ses données de santé; l'impossibilité de déduire de ces données à caractère personnel relatives à la santé des données de contenu relatives à la santé; l'impossibilité du couplage de données de santé avec d'autres données à caractère personnel comme les données sociales et fiscales, qui sera garantie par "la structure même de la plate-forme qui ne constituera pas un lieu de concentration des données mais bien un filtre qui répartira chaque donnée entre de nombreux utilisateurs tout en contrôlant leur accès à ces informations"; ou encore le contrôle et la limitation, fonctionnelle et temporelle, de l'accès des acteurs aux données[278].

---

[276] Journal du Médecin TV, 15 juillet 2008, http://fr.medisurf.be/protected/archives/WebTV/Archief/20080715.html.

[277] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 39-40, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[278] Rapport fait au nom de la Commission des Affaires sociales, par M. Brotchi, Sénat, 15 juillet 2008, Doc. n° 4-863/2, http://www.senate.be/www/?MIval=/index_senate&MENUID=12410&LANG=fr.

E. Les critiques adressées du point de vue juridique

Yves Poullet, juriste des Facultés universitaires Notre Dame de la Paix à Namur, a lui aussi été entendu devant la Commission de la Santé publique, et adresse au projet eHealth un certain nombre de critiques d'ordre juridique.

D'une manière générale, Y. Poullet note que de nombreux revirements de volonté du gouvernement sont présents dans le projet eHealth, sans pour autant être dûment justifiés. En effet, lors de l'avant-projet de loi relatif à la télématique médicale, l'indépendance du secteur de la santé par rapport à celui de la sécurité sociale était promue, se manifestant entre autres par la volonté de créer un numéro d'identification propre au système de santé, différent de celui du registre national, ainsi que la création d'un comité sectoriel propre. Or, l'actuel projet eHealth consacre, à l'inverse, un lien étroit entre ces deux secteurs, en optant pour l'utilisation du numéro d'identification du registre national, pour la création d'une section santé au sein du comité sectoriel de la sécurité sociale et de la santé, créé auprès de la BCSS – ce qui limite son autonomie –, et en prévoyant d'étroites relations avec la BCSS. Y. Poullet dénonce cette absorption du secteur de la santé par celui de la sécurité sociale, se manifeste encore dans le fait qu'eHealth soit à considérer comme une institution publique de sécurité sociale et non comme une institution publique de la santé publique. De plus, cette invasion de la sécurité sociale se cristallise dans la disposition du projet de loi qui confie la gestion journalière de la plate-forme à l'administrateur général de la BCSS, ce qui implique que ce dernier sera "aux commandes des deux traitements de données à caractère personnel les plus importants de Belgique"[279]. L'expert se pose alors la question de savoir si ce phénomène démontre une rationalisation ou s'il cache une finalité de traitement moins heureuse. Il va jusqu'à parler d'une érosion de la dimension santé de la plate-forme BeHealth depuis 2006 au profit de la dimension instrument de contrôle des dépenses de santé[280].

Une seconde critique adressée par Y. Poullet concerne les règles de concurrence, lesquelles ne seraient pas respectées par le projet de loi. En effet, si certaines des missions d'eHealth doivent être assumées par une institution publique – comme la transmission de données à d'autres institutions –, il en est d'autres, en revanche, qui peuvent être fournies par des acteurs privés, telles que la messagerie privée sécurisée entre médecins, l'accès à des banques de données de patients, le codage de données en vue de la recherche, ou encore le rôle d'organisme intermédiaire. Selon l'expert, "il est à craindre que ces activités concurrentielles ne puissent aisément se développer au vu des règles qui imposent le passage par le système eHealth et des avantages qui résultent de sa subsidiation publique"[281].

---

[279] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 36, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[280] Journal du Médecin, 26 juin 2008, in http://www.medisurf.be/

[281] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 37, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

En outre, la répartition des compétences est problématique, étant donné que la compétence de recherche en matière de soins de santé appartient aux entités fédérées, alors que le projet eHealth insiste sur sa mission en tant qu'organisme intermédiaire pour la recherche et l'élaboration d'une politique des soins de santé. De plus, "le projet intervient à un niveau tant préventif que thérapeutique, ce qui implique également deux niveaux de compétence, à savoir le pouvoir fédéral et les pouvoirs fédérés"[282]. Y. Poullet recommande alors l'adoption d'une disposition délimitant clairement le champ d'application du projet de loi, sans quoi le législateur fédéral se rendrait coupable d'un dépassement de ses compétences.

S'ajoutent à ces critiques des considérations relevant de la protection de la vie privée et de l'application de la loi du 8 décembre 1992 y relative, qui ne serait pas respectée, selon l'expert, en différents aspects. Tout d'abord, les finalités de la plate-forme, telles que décrites à l'article 4 du projet de loi, sont loin d'être précises et déterminées. Ensuite, l'utilisation du numéro d'identification du registre national est disproportionnée dans les applications entre médecins offertes par la plate-forme, les arguments avancés pour justifier cette solution, bien que retenus par la CPVP optant pour un revirement de jurisprudence en la matière, étant "peu probants (risques d'erreur et de coûts) au regard des risques encourus par l'utilisation d'un numéro unique". L'expert ajoute que "la Belgique est le seul pays à prendre le risque de l'utilisation d'un numéro unique y compris en matière de flux de données de santé et à imposer pour tout passage par l'infrastructure eHealth l'utilisation de ce numéro, ce qui est disproportionné et générateur de risques d'atteinte à la protection des données lorsqu'il s'agit de communications entre prestataires de soins"[283]. L'argument en faveur d'eHealth soutenant que la plate-forme ne conservera aucune donnée à caractère personnel outre les données d'identité est, selon Y. Poullet, difficilement soutenable, étant donné que " le répertoire de références qui permet de savoir où se trouvent les dossiers relatifs à telle personne est un traitement très sensible dans la mesure où il permet de déduire en fonction de la nature de l'endroit, les caractéristiques de santé de la personne"[284]. De même, la subordination de l'inscription du patient au répertoire de référence à son consentement est un leurre, ce dernier risquant grandement d'être faussé, et l'obligation d'information du patient au sujet des personnes ayant accès à ses données risquant de ne pas être dûment remplie en pratique. En effet, les données du patient subiront différents traitements, le premier par son médecin, le second par l'établissement de soin, le suivant par eHealth et les autres par des personnes non encore déterminées. Or, la loi du 8 décembre 1992 n'autorise que les traitements ultérieurs aux finalités compatibles avec celles du traitement initial, les autres traitements nécessitant d'informer le patient et d'obtenir son consentement spécifique. Y. Poullet regrette que la loi n'aborde pas la question de la compatibilité des différents traitements envisageables, laissant sans

[282] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 38, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[283] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 38-39, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[284] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 39, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

réponse la problématique du consentement sur un point de plus. Dernière préoccupation relevant de la vie privée, l'expert recommande qu'une référence soit faite au nécessaire respect du secret médical, et que la confusion entre la notion de confidentialité et celle de secret professionnel (art. 458 du Code pénal) soit levée par une référence à ce dernier. En effet, "cette référence à l'article 458 du Code pénal garantira le silence des personnes intervenant dans les traitements qui seront opérés par et grâce à eHealth"[285].

L'expert clôture son audition par deux dernières remarques, l'une tenant à la question du respect de la loi belge et de la directive européenne en matière de libre prestation des services; l'autre regrettant l'absence de toute représentation des patients dans la gestion de la plate-forme, ceux-ci étant pourtant des acteurs centraux de la problématique de la santé.

§ 5. – Les justifications avancées par les créateurs du projet et leurs réponses aux critiques adressées à celui-ci

A l'origine du projet eHealth se trouve Frank Robben, administrateur général de la BCSS et fondateur du projet. Que ce soit lors de sa présentation de la plate-forme auprès de différents acteurs du secteur de la santé, ou au cours de son audition devant la Commission de la santé publique de la Chambre des représentants, il expose un certain nombre d'arguments en faveur de la création d'eHealth. Mais il n'est pas le seul à défendre ce projet, divers parlementaires se joignant à son opinion, tout comme c'est le cas du Collège intermutualiste national. En outre, la Ministre Onkelinx répond également aux critiques adressées à ce projet, étant donné que c'est elle qui l'a proposé au Conseil des Ministres.

Certaines des justifications avancées par ces différentes personnes reprennent les arguments présentés dans l'exposé des motifs du projet de loi, et tiennent entre autres aux objectifs de celui-ci, ou encore au caractère décentralisé de la plate-forme eHealth. Nous ne reprendrons pas ces justifications ici, étant donné qu'elles ont été présentées au cours du second paragraphe de cette section. Nous nous contenterons donc d'analyser dans les lignes qui suivent les réponses apportées par les créateurs et défenseurs du projet aux diverses critiques y adressées, ces critiques ayant été exposées durant le paragraphe précédent.

A. Caractère facultatif de la plate-forme eHealth

A de nombreuses reprises, F. Robben et d'autres défendeurs du projet rappellent le caractère non obligatoire de la plate-forme eHealth, chaque utilisateur décidant librement de s'y inscrire ou non. La justification réside dans le fait qu'eHealth ne pourra fonctionner qu'à condition de gagner la confiance des destinataires, et que le meilleur moyen pour ce faire est de rendre le système facultatif. Cela n'est pas le cas du système

[285] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 40, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

de la BCSS, mais le caractère obligatoire de celui-ci "trouve son fondement dans des raisons propres à la nature de la sécurité sociale"[286].

Plusieurs parlementaires insistent toutefois sur l'importance de gagner la confiance des futurs utilisateurs de la plate-forme, son caractère facultatif induisant le risque qu'elle ne soit qu'une coquille vide si aucun prestataire ne s'y inscrit et n'en fait usage. Rappelons en outre que, selon M. Moens de l'Absym, ce caractère facultatif demeure hypothétique en raison des larges compétences et facultés octroyées à la plate-forme eHealth.

B. Respect et soutien des initiatives locales, et absence de tout monopole

Aux critiques selon lesquelles eHealth ne prendrait pas en considération les initiatives locales d'échange électronique de données, et ne respecterait pas les règles en matière de concurrence, F. Robben répond en déclarant que "la plate-forme eHealth respecte et soutient les initiatives locales ou régionales existantes en matière de collaboration électronique dans les soins de santé (Réseau Santé Wallon, Abrumet, etc.) et les initiatives privées en matière de prestation de services électroniques aux acteurs des soins de santé"[287]. Il déclare également que des discussions ont eu lieu avec ces différents acteurs, mais de manière informelle puisque eHealth n'existe pas encore[288]. Notons toutefois que P. Olivier, représentant du RSW devant la Commission de la santé publique, conteste avoir été associé à l'élaboration du projet de loi, déclarant au contraire que ses contacts avec les promoteurs d'eHealth sont très récents, ce qui est dommage, selon lui, étant donné la pertinence d'une concertation "compte tenu de l'impératif de développer des normes techniques compatibles entre les systèmes"[289].

S'agissant des initiatives locales ou régionales, le créateur de la plate-forme eHealth déclare que celle-ci souhaite non seulement les respecter, mais en outre les encourager, les coordonner et les soutenir. Il s'agit de favoriser les initiatives de collaboration, raison pour laquelle eHealth propose de manière généralisée des services de base électroniques ainsi que le développement de standards en matière de technologies de l'information et de la communication. F. Robben exprime sa volonté de rendre ces initiatives locales et régionales "interopérables entre elles, de sorte que les prestataires de soins, les établissements de soins et les patients puissent obtenir accès, à travers toutes

[286] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 56, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[287] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 3, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[288] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 55, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[289] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 61, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

ces initiatives locales et régionales, aux données à caractère personnel pertinentes auxquelles ils sont autorisés à avoir accès"[290].

Quant aux relations d'eHealth avec les sociétés privées, au sujet desquelles les critiques rendent eHealth coupable de concurrence déloyale et de monopole, F. Robben précise qu'eHealth "se limite à offrir les services de base prévus dans le projet de loi et ne développera donc par exemple pas de logiciels pour la gestion de dossiers médicaux. Les services de base proposés par la plate-forme eHealth sont disponibles pour tous les acteurs des soins de santé, donc également pour les instances qui offrent des services de technologie de l'information et de la communication aux prestataires et établissements de soins. Ceux-ci peuvent les utiliser à l'appui de leur prestation de services. Les services de base proposés par la plate-forme eHealth sont pour la plupart développés en ayant recours à des sociétés privées, choisies sur la base d'un marché public. La plate-forme eHealth définit uniquement des standards en matière de technologies de l'information et de la communication et ce exclusivement dans des domaines où elle n'intervient pas en tant que fournisseur de services. Ainsi il n'y a pas de concurrence déloyale"[291].

C. Sécurité et protection de la vie privée

Ainsi que nous l'avons mentionné ci-dessus, les associations de prestataires de soins reprochent aux auteurs du projet eHealth de consacrer davantage d'importance à l'efficacité des échanges, à la gestion de l'assurance-maladie, au soutien à la politique des soins de santé, et à la connaissance des dossiers patients par les mutuelles, au détriment de la confidentialité, et sans garantir le respect des deux conditions essentielles à l'existence de la plate-forme eHealth, à savoir la sécurité et la confiance[292]. Selon F. Robben, au contraire, "une attention particulière est réservée à la sécurité de l'information et à la protection de la vie privée. Un chiffrage des données à caractère personnel relatives à la santé échangées entre l'expéditeur et le destinataire peut être organisé de manière telle que la plate-forme eHealth n'est pas en mesure de voir les données de santé échangées. La plate-forme eHealth est pourvue d'un contrôle d'accès préventif poussé, à travers la détermination des prestataires de soins ou des établissements de soins qui peuvent obtenir communication, dans quelles situations, de quels types de données, concernant quels types de patients et pour quelles périodes. Un système permet d'exécuter le contrôle d'accès de façon efficace et préventive. Des données à caractère personnel relatives à la santé ne peuvent être échangées à travers la plate-forme eHealth que moyennant une autorisation accordée par la loi, par le Comité sectoriel de la santé ou par le patient. La législation en matière de protection de la vie

[290] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 10, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.
[291] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 10, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.
[292] Voy. *supra*, réaction de l'Absym.

privée, de droits du patient et d'exercice de la médecine est appliquée sans restriction"[293]. La ministre confirme, devant le Sénat, ces propos, en rappelant que seules "les personnes autorisées ont accès au réseau. De plus, le réseau est sécurisé par un système de log-in et l'accès au réseau ne donne aucun accès aux données médicales si elles ne sont pas communiquées par le médecin ou par l'institution qui les détient. Enfin, les données qui transitent par la plate-forme seront cryptées. La plate-forme permet donc de posséder un système bien plus sécurisé que le système actuel où toutes les données confidentielles se trouvent dans un dossier sur papier, voire dans un courrier électronique"[294]. A la considération selon laquelle des risques importants sont ouverts par l'échange de données via des supports papier, M. De Maght (LDD) ajoute que "nos soins de santé ont en fait besoin d'un système numérique car, à l'heure actuelle, il y a un trop grand gaspillage de papier"[295]; tout en se montrant pour le reste très critique à l'égard du projet eHealth.

Plus particulièrement, F. Robben fait état de diverses mesures visant à éviter l'agrégation illégitime de données à caractère personnel relatives à la santé, à savoir: "l'enregistrement décentralisé de données à caractère personnel relatives à la santé; l'exigence d'une autorisation préalable pour l'échange de données à caractère personnel relatives à la santé accordée par la loi, le Comité sectoriel de la santé ou le patient; le contrôle de la légitimité de l'échange de données à caractère personnel relatives à la santé à travers la plate-forme eHealth est effectué par un médecin, un conseiller en sécurité de l'information et le Comité sectoriel de la santé; le codage des données à caractère personnel échangées relatives à la santé entre l'expéditeur et le destinataire; une solide gestion des utilisateurs et des accès; le logging de l'action d'échanger des données à caractère personnel relatives à la santé, et non des données à caractère personnel en tant que telles". De plus, le fondateur du projet entend la demande des chercheurs scientifiques requérant un système de codage et d'anonymisation des données à caractère personnel relatives à la santé, "qui ne permette pas de déduire de façon directe ou indirecte l'identité du patient et/ou du prestataire de soins". Il ajoute que "le codage ou l'anonymisation est plus que le codage d'une clé d'identification: il faut faire en sorte qu'il soit impossible de déduire l'identité du patient ou du prestataire de soins à partir de la combinaison des données"[296].

Quant aux craintes exprimées par les associations de médecins au sujet de la modification, par le projet de loi, des règles relatives au consentement, à la traçabilité de la consultation ainsi qu'à la communication des données, la ministre tente de les rassurer en précisant que ce projet ne modifie en rien la situation existante à ce sujet. En effet, "la traçabilité des consultations est assurée par un répertoire de référence pour chaque patient

---

[293] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 3-4, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[294] Rapport fait au nom de la Commission des Affaires sociales, par M. Brotchi, Sénat, 15 juillet 2008, Doc. n° 4-863/2, http://www.senate.be/www/?MIval=/index_senate&MENUID=12410&LANG=fr.

[295] Comte rendu analytique de la séance plénière de la Chambre des Représentants du 10 juillet 2008, Doc. n° 0050, p. 47, http://www.lachambre.be/doc/PCRA/pdf/52/ap050.pdf.

[296] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 8, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

et qui indique clairement qui a eu accès à quelles données. Ce répertoire est d'ailleurs accessible tant au médecin traitant qu'au patient"[297].

A ces justifications d'ordre technique s'ajoute la considération selon laquelle un système développé à l'échelon national serait plus protecteur de la vie privée, ou en tout cas plus en mesure de garantir la sécurité des échanges électroniques, que ne peuvent le faire les différents systèmes locaux développés dans divers hôpitaux et autres institutions du secteur des soins de santé. En effet, selon B. Van den Bosch, directeur des systèmes d'information des UZ Leuven, "un incident de sécurité provoqué par une application mal sécurisée à un endroit sur le terrain a une influence négative sur toutes les applications télématiques, même celles qui sont bien sécurisées, de sorte que l'échange électronique d'informations (médicales) est systématiquement remis en cause dans les médias. En proposant une solution de qualité à tout un chacun, on coupe court à toute propension au bricolage"[298].

D. Relation avec la BCSS

Nombreuses sont les critiques concernant le manque d'indépendance de la plate-forme eHealth, celle-ci étant liée, de manière exagérée selon certains, à la BCSS. F. Robben conteste ce point de vue, en déclarant que "si la plate-forme eHealth profite du *know-how* de la Banque-Carrefour de la Sécurité Sociale en matière d'organisation d'échanges électroniques de données, elle dispose cependant d'une infrastructure propre, indépendante de celle de la Banque-carrefour"[299]. Il ajoute qu' "à aucun moment, il n'a été procédé de confusion entre les organes de gestion et les organes de contrôle de la plate-forme. Une incompatibilité a expressément été prévue entre une fonction au sein de la plate-forme eHealth et une fonction au sein du comité sectoriel". Une autre garantie d'indépendance, selon l'auteur du projet, est créée au sein de la Commission de la protection de la vie privée, dont "parmi les seize membres, quatorze occupent une autre fonction. Une règle empêche qu'un membre codécide dans un dossier qui le concerne"[300].

La justification de la création de la plate-forme eHealth au sein de la BCSS réside, selon l'exposé des motifs, dans la volonté de réutiliser ce qui existe déjà et qui fonctionne bien, ainsi que de garantir une certaine unité en termes de direction[301].

---

[297] Rapport fait au nom de la Commission des Affaires sociales, par M. Brotchi, Sénat, 15 juillet 2008, Doc. n° 4-863/2, http://www.senate.be/www/?MIval=/index_senate&MENUID=12410&LANG=fr.

[298] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 35, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[299] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 4, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[300] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 55, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[301] Voy. *supra,* § 2, A, de cette section.

E. Représentation de tous les acteurs des soins de santé, et volonté de les impliquer

Bon nombre des critiques adressées au projet eHealth émanent d'acteurs de terrain, représentants de médecins principalement, qui reprochent aux auteurs du projet de ne pas les avoir concertés en temps voulu. Ils se sentent "mis devant le fait accompli", et impuissants à réagir de manière adéquate en si peu de temps. Devant la Commission de la santé publique, la ministre Onkelinx "s'oppose à tous ceux qui prétendent qu'il y aurait eu un manque de contacts préparatoires". Elle cite d'ailleurs divers exemples de consultation des acteurs concernés par le projet, dont "les réunions du 'groupe vision' dans le cadre médico-mutualiste, plusieurs contacts entre les intervenants des différentes sensibilités avec ses collaborateurs, la présentation officielle du projet dans les organes de l'INAMI, une réunion informelle le 14 avril 2008 avec le Réseau Santé Wallon, une autre le 16 avril 2008 avec un représentant de la Région de Bruxelles-Capitale, etc."[302]. Il demeure toutefois étrange que les acteurs du secteur de la santé se sentent à ce point exclus et mis à l'écart de ce projet, malgré cette concertation préalable prétendue par la ministre.

Au-delà de leur implication dans la préparation du projet, les auteurs de celui-ci déclarent vouloir permettre aux acteurs de terrain de participer non seulement à l'exécution du projet et à la mise en place de la plate-forme par des arrêtés d'exécution – arrêtés qui, selon les dires de la ministre "devront être le fruit d'une concertation avec l'ensemble des professionnels"[303] –, mais aussi au fonctionnement d'eHealth. Ainsi, ils affirment que "la plate-forme eHealth est gérée par des représentants des divers acteurs des soins de santé. Le contrôle du fonctionnement sécurisé de la plate-forme eHealth est opéré par le Comité sectoriel de la santé, composé de deux personnes de la Commission de la protection de la vie privée (qui ne participent pas à la gestion opérationnelle de la plate-forme eHealth) et de médecins désignés par la Chambre des représentants. Les autorisations pour les échanges de données relatives à la santé sont octroyées par ce comité"[304].

De plus, l'ASBL qui peut être créée en vue de gérer certains flux de données "intègre des représentants de toutes les parties concernées. Elle offre une structure au sein de laquelle les spécialistes de toutes origines sont impliqués. Elle est contrôlée majoritairement par les médecins. La Commission estime avoir suffisamment de garanties que cette association respectera les impératifs liés à la vie privée"[305].

---

[302] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 77, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[303] Rapport fait au nom de la Commission des Affaires sociales, par M. Brotchi, Sénat, 15 juillet 2008, Doc. n° 4-863/2, http://www.senate.be/www/?MIval=/index_senate&MENUID=12410&LANG=fr.

[304] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 4, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[305] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 60, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

Notons enfin qu'un souci de respect de la liberté thérapeutique est affirmé de manière claire, mais peu explicitée : "la plate-forme eHealth respecte la liberté thérapeutique des prestataires de soins"[306].

F. Des services à valeur ajoutée

Frank Robben, dans un article publié par la revue *citizene* en mars 2008, parle de services à valeur ajoutée offerts par l'informatisation de certains échanges et opérations, et donc potentiellement par la plate-forme eHealth[307]. Parmi ceux-ci, il relève entre autres le réseau Carenet, l'identification et l'authentification de l'identité de l'utilisateur grâce à la carte d'identité électronique ou à l'usage de token, la boîte aux lettres électronique, la transmission de factures du tiers payant par voie électronique, l'application de Medic-e, ou encore la Fondation Registre du Cancer.

Le Collège intermutualiste national, semble rejoindre cet opinion, constatant "que tous les acteurs des soins de santé passent des accords portant sur un échange d'informations à la fois transparent et sécurisé", et citant à titre d'exemple "la collaboration entre la plate-forme eHealth et l'association eCare qui a permis une simplification administrative grâce à la suppression des documents papiers rendue elle-même possible par des applications en ligne". A ce sujet, "eHealth ouvre également des perspectives au patient en lui permettant de consulter lui-même certaines données"[308].

G. Réputation internationale et européenne de la Belgique

La réputation internationale et européenne de la Belgique semble également constituer un argument en faveur du projet eHealth, notre pays pouvant de la sorte être présenté comme un exemple de système d'information à la pointe des progrès technologiques. F. Robben y fait en effet allusion[309], en déclarant que le modèle belge de la BCSS est actuellement une référence, comparable au modèle danois d'échange d'informations relatives aux soins de santé, qui est souvent cité comme exemple européen. De tels développements, réalisés à l'intention de la BCSS, pourraient également être utilisés pour la plate-forme eHealth.

Notons que cette importance de rendre la Belgique pionnière en matière de soins de santé est également manifeste au travers des différentes considérations rendues au sujet de l'utilisation du numéro d'identification du registre national dans le secteur de la santé.

---

[306] Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, p. 4, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.

[307] DECHAMPS, F.R., "Frank Robben. De knowhow van de sociale sector ten dienste van de volksgezondheid", *Citizene*, februari-maart, nummer 01 2008.

[308] Comte rendu analytique de la séance plénière de la Chambre des Représentants du 10 juillet 2008, Doc. n° 0050, p. 31, http://www.lachambre.be/doc/PCRA/pdf/52/ap050.pdf.

[309] DECHAMPS, F.R., "Frank Robben. De knowhow van de sociale sector ten dienste van de volksgezondheid", *Citizene*, februari-maart, nummer 01 2008.

§ 6. – Les amendements et garde-fous apportés au projet

Si le Sénat n'a apporté aucun amendement au projet de loi transmis par la Chambre des Représentants, celle-ci avait auparavant quelque peu modifié le texte initialement déposé, et ce dans le but de répondre aux critiques des acteurs des soins de santé, et de les rassurer.

A. La définition des données à caractère personnel relatives à la santé

Un premier amendement proposé le 1er juillet par M. Goutry (CD&V - N-VA) et consorts vise à inclure, à l'article 3 du projet de loi – article énonçant diverses définitions, afin de mettre tout le monde d'accord sur ce qu'il convient d'entendre par les notions clés du projet –, un 9° énonçant une définition des données à caractère personnel relatives à la santé. Selon les parlementaires à l'initiative de la proposition d'amendement, une telle définition serait utile à inclure dans la loi, et devrait être formulée de la sorte: "toutes données à caractère personnel dont on peut déduire une information sur l'état antérieur, actuel ou futur de la santé physique ou psychique de la personne identifiée ou identifiable, à l'exception des données purement administratives ou comptables relatives aux traitements ou aux soins médicaux"[310]. Cette définition diffère quelque peu de celle adoptée par la loi relative à la protection de la vie privée, qui ne retient comme données relatives à la santé que celles qui concernent directement l'état de santé, et non toutes celles qui révèlent l'état de santé. L'on peut regretter qu'aucune précision n'ait été apportée, trois termes différents – à savoir "concerner", "révéler" et "déduire" – étant au total empruntés dans ces deux lois, sans qu'aucune clarification n'indique leur distinction. L'avantage de l'insertion de cette définition est d'exclure expressément du champ d'application du projet de loi les données à caractère administratif. Seules les données personnelles à caractère médical demeurent concernées.

B. La gratuité des services de base

Un second amendement, proposé par les mêmes personnes et lui aussi retenu, précise que les services de base de la plate-forme, visés dans le cadre de la mission prévue à l'article 5, 4° du projet de loi, seront mis à disposition des acteurs des soins de santé gratuitement. Les auteurs de l'amendement précisent que "la mise à la disposition gratuite concerne uniquement la plate-forme électronique standard et les services de base électroniques standard. Au cas où des adaptations spécifiques doivent être réalisées pour certains acteurs des soins de santé ou des moyens humains doivent être engagés pour utiliser les services, les frais y relatifs peuvent toutefois être facturés aux utilisateurs"[311]. Au sein de cette même mission, le point b) de l'article 5, 4° énonce une liste de ces services de base, à laquelle est ajouté "un système de cryptage des données entre

[310] Amendement n° 1 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[311] Amendement n° 2 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.

l'expéditeur et le destinataire". Ce système de cryptage "signifie que les données, dans la mesure où elles ne sont pas nécessaires au routage correct des données de contenu, sont cryptées au moment de leur envoi et ne peuvent être décryptées qu'auprès du destinataire de sorte qu'il puisse prendre connaissance des informations originales. La plate-forme *eHealth* ne peut donc pas prendre connaissance des données cryptées. Avant d'accorder une autorisation pour l'échange de données à caractère personnel, le comité sectoriel examinera si un tel cryptage est nécessaire et, le cas échéant, il imposera ce cryptage en tant que modalité de l'échange des données". Au sein du même article, il est également ajouté que "l'implémentation du répertoire de références ne pourra être réalisée qu'après avis de la section santé du comité sectoriel de la sécurité sociale et de la santé"[312].

C. Les garanties supplémentaires entourant la mission d'organisme intermédiaire de la plate-forme eHealth

Une autre mission de la plate-forme eHealth, attribuée par l'article 5, 8° du projet de loi, concerne son rôle d'organisme intermédiaire selon lequel elle coderait les données pour les mettre à disposition de destinataires en vue de la recherche à des fins historiques, statistiques et scientifiques. Ainsi que nous l'avons mentionné ci-dessus, cette mission est relativement contestée par certains opposants au projet de loi, ce qui a justifié l'ajout d'une garantie supplémentaire, à savoir: "la plate-forme eHealth peut uniquement réaliser cette mission à la demande d'une chambre législative, d'une institution de sécurité sociale, de la fondation visée à l'article 45*quinquies* de l'arrêté royal n° 78 du 10 novembre 1967 relatif à l'exercice des professions de soins de santé, de l'Agence intermutualiste, du Centre fédéral d'expertise des soins de santé, de l'association sans but lucratif visée à l'article 37, d'un ministre fédéral, d'un service public fédéral ou d'une institution publique dotée de la personnalité juridique qui relève des autorités fédérales; le Roi peut, par arrêté délibéré en Conseil des ministres et après avis de la Commission de la protection de la vie privée et du Comité de gestion, élargir la liste des instances qui peuvent faire appel à la plate-forme *eHealth* comme organisation intermédiaire"[313]. Les catégories d'instances pouvant demander à la plate-forme d'exécuter cette mission sont de la sorte limitées, tout en reconnaissant la possibilité d'élargir cette liste par arrêté royal.

D. Les précisions au sujet de l'autorisation de la section santé du comité sectoriel de la sécurité sociale et de la santé, et la création de cette dernière

L'article 11 du projet de loi soumet toute communication de données à une autorisation de principe de la section santé du comité sectoriel compétent en la matière. L'alinéa 3 de cet article précise qu'avant d'accorder son autorisation, la section santé devra vérifier la conformité de la communication à la loi et à la protection de la vie

[312] Amendement n° 3 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[313] Amendement n° 4 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.

privée. L'amendement n° 5[314] propose d'ajouter qu'une attention particulière devra être prêtée au cryptage éventuel des données à caractère personnel en question, afin de déterminer si un tel cryptage est nécessaire en l'espèce, précision qui a été retenue et qui figure donc dans le texte approuvé par les chambres législatives. L'amendement suivant concerne la même disposition du projet de loi, et précise que cette autorisation doit être donnée préalablement, soumettant la réalisation de la communication de données en question à l'octroi de l'autorisation. La communication ne peut donc avoir lieu avant l'obtention de l'autorisation. De plus, la possibilité est offerte d'assortir l'autorisation de modalités et de règles particulières à respecter lors de la réalisation de la communication. Une précision est également apportée au sujet des communications ayant débuté avant l'entrée en vigueur de la loi: " Dans la mesure où une communication est déjà opérationnelle avant l'entrée en vigueur de la présente loi (c'est-à-dire à un moment où elle n'exigeait pas encore d'autorisation de la part de la section santé), la section santé doit accorder une autorisation dans l'année pour cette communication. Ceci signifie que les flux de données à caractère personnel opérationnels pour lesquels la section santé ne devait pas accorder d'autorisation avant l'entrée en vigueur de la présente loi, peuvent être poursuivis pour autant qu'ils soient entérinés dans l'année par la section santé"[315].

La justification de cet amendement précise que tout cela suppose la création de la section santé du comité sectoriel de la sécurité sociale et de la santé. Certains interprètent cela comme une garantie de l'instauration de cet organe, ce qui nous semble toutefois un peu léger. La ministre elle-même l'a déclaré lors de la séance plénière tenue à la Chambre des représentants le jeudi 10 juillet, en ces termes: "tout nouveau flux de données est conditionné à la création de la chambre Santé du comité sectoriel de la sécurité sociale"[316].

E. La composition du Comité de gestion, le contrôle de la plate-forme eHealth et le Comité de concertation

Quelques modifications sont apportées à l'article 15 concernant le Comité de gestion. Tout d'abord, il est précisé que le président a voix délibérative, et que l'organe se compose de 31 membres. Ensuite, une modification plus substantielle concerne la nomination des sept représentants des prestataires de soins et des établissements de soins ayant voix délibérative au sein de ce Comité, qui seront désormais proposés par les représentants des prestataires de soins et des établissements de soins au sein du Comité d'assurance des soins de santé de l'Institut national d'assurance maladie invalidité, et non par l'ensemble du Comité d'assurance[317].

Quant au contrôle de la plate-forme eHealth, si le texte initial du projet de loi imposait qu'il soit exercé par les mêmes commissaires du gouvernement et par le même

[314] Amendement n° 5 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[315] Amendement n° 6 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[316] Comte rendu analytique de la séance plénière de la Chambre des Représentants du 10 juillet 2008, Doc. n° 0050, p. 49, http://www.lachambre.be/doc/PCRA/pdf/52/ap050.pdf.
[317] Amendement n° 8 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.

réviseur que ceux qui exercent la surveillance pour la BCSS, le texte final retenu par les assemblées législatives n'impose pas cette identité de contrôleurs[318].

S'agissant du Comité de concertation des utilisateurs, le texte amendé précise qu'il est présidé par un médecin, ce qui est jugé souhaitable étant donné la mission qui lui est attribuée[319].

Dans le même ordre d'idées, plusieurs amendements augmentent le nombre de médecins membres du comité sectoriel de la sécurité sociale et de la santé[320].

F. L'évaluation de la loi deux ans après son entrée en vigueur

Les parlementaires ont en outre estimé "souhaitable de prévoir un système de contrôle parlementaire *a posteriori* concernant l'application de la présente loi. À cet effet, il est prévu que les ministres compétents pour la santé publique, les affaires sociales et l'informatisation de l'état rendent compte de l'application de la présente loi auprès des chambres législatives deux ans après l'entrée en vigueur de la présente loi et formulent éventuellement des recommandations afin d'améliorer cette application. Le rapport des ministres est basé sur les rapports d'évaluation de la plate-forme eHealth elle-même et de la section santé du comité sectoriel de la sécurité sociale et de la santé"[321].

Section III. – Conclusion

Le projet eHealth présente plusieurs aspects bénéfiques pour le secteur des soins de santé, et ne semble pas nécessairement devoir être rejeté dans son ensemble. Simplement, la rapidité et l'obscurité qui entourent sa création inspirent la méfiance des acteurs concernés, ce qui est aisément compréhensible. De plus, le projet contient encore des aspects flous voire des lacunes, qu'il convient de corriger et de préciser en concertation avec les acteurs concernés.

Les auteurs du projet et les parlementaires semblent avoir pris conscience des problèmes et critiques adressés à eHealth, et affirment être soucieux d'y remédier en impliquant pleinement les acteurs de terrain dans la mise en œuvre de la plate-forme par les arrêtés royaux d'exécution, ainsi que dans sa gestion et son fonctionnement. Il ne nous reste qu'à espérer qu'ils tiendront leurs engagements, et qu'eHealth constituera un outil sécurisé et efficace plutôt qu'un *Big brother* tant craint et peu désirable.

---

[318] Amendement n° 7 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[319] Amendement n° 9 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[320] Amendements n° 10 et 11 déposés par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
[321] Amendement n° 12 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.

Chapitre II. – L'utilisation du numéro du Registre national des personnes physiques

Section Ière. – La loi du 8 août 1983 organisant un Registre national des personnes physiques

§ 1er. – Accès aux informations enregistrées et conservées par le Registre national

La loi relative au Registre national prévoit la possibilité d'obtenir l'accès à ce registre. Cet accès est accordé par le Comité sectoriel du Registre national[322], la loi énonçant de manière limitative les catégories de personnes et autorités bénéficiant de cette possibilité d'accès. Il s'agit des autorités publiques belges pour les informations qu'elles sont habilitées à connaitre en vertu de la loi, décret ou ordonnance; des organismes publics ou privés pour l'accomplissement de tâches d'intérêt général confiées par loi, décret ou ordonnance; des sous-traitants – qu'il s'agisse de personnes physiques ou morales – des deux premiers destinataires, qui exercent sous le contrôle de ceux-ci et qui doivent respecter la loi de 1992 relative à la protection de la vie privée; des notaires et huissiers de justice; de l'Ordre des pharmaciens et enfin de l'Ordre des barreaux.

Avant d'autoriser l'accès au registre national, le comité vérifie, en vertu du principe de finalité qui domine l'ensemble des législations concernant la protection de la vie privée, que les finalités pour lesquelles les informations sont demandées, sont déterminées, explicites et légitimes. Il vérifie également que les données demandées sont adéquates, pertinentes et non excessives par rapport à ces finalités. En outre, le respect des lois relatives au Registre national et à la protection de la vie privée doit être contrôlé, ainsi que celui de leurs dispositions d'exécution.

Une fois l'accès obtenu, les autorités autorisées à consulter les données du Registre national ne peuvent plus les requérir auprès de la personne concernée. Elles ont en outre l'obligation de désigner un consultant en sécurité de l'information et en protection de la vie. Afin d'assurer une certaine transparence et publicité, un registre des autorisations est tenu par la Commission de la protection de la vie privée, et rendu accessible au public. Cela permet à toute personne de savoir exactement qui a accès à ses données.

Une exception au principe d'autorisation de l'accès aux informations contenues dans le registre national est toutefois prévue, le Roi ayant la possibilité de déterminer par arrêté royal les cas dans lesquels l'autorisation n'est pas requise. Le Roi a usé de cette faculté offerte par la loi, dont voici quelques exemples:

---

[322] Notons qu'auparavant, une longue procédure requérait l'adoption d'un arrêté royal pour autoriser l'accès au registre. Maintenant, depuis l'adoption de la loi du 25 mars 2003, c'est à la CPVP qu'il convient de s'adresser, et plus particulièrement à son Comité sectoriel du Registre national. http://www.ibz.rrn.fgov.be/index.php?id=154&L=0.

- Arrêté royal du 29 juin 2003 organisant l'accès aux informations et l'usage du numéro d'identification du Registre national des personnes physiques dans le chef de la direction de la Stratégie Clients de la Société des Transports intercommunaux de Bruxelles;
- Arrêté royal du 2 mai 2002 modifiant l'arrêté royal du 30 mai 1994 autorisant la Société terrienne flamande à accéder aux informations et à utiliser le numéro d'identification du Registre national des personnes physiques.
- Arrêté royal du 3 septembre 2000 autorisant l'Institut bruxellois francophone pour la Formation professionnelle à accéder aux informations et à utiliser le numéro d'identification du Registre national des personnes physiques.

§ 2. – Autorisation d'utilisation du numéro d'identification du Registre national

La loi relative au registre national prévoit non seulement la possibilité, pour certaine personnes ou autorités et moyennant l'autorisation du Comité sectoriel, d'accéder à certaines informations contenues dans le registre national, mais également la possibilité d'en utiliser le numéro d'identification. Pour ce faire, une autorisation doit également être octroyée par le Comité sectoriel du Registre national, cette possibilité se limitant aux mêmes personnes et autorités que celles pouvant jouir de l'accès au registre.

La loi offre une garantie supplémentaire, en énonçant l'interdiction d'utiliser ce numéro sans autorisation, ou à d'autres fins que celles pour lesquelles l'autorisation a été accordée. En revanche, les personnes et autorités autorisées à utiliser ce numéro sont obligées de le faire dans le cadre des contacts qu'elles entretiennent avec le Registre national des personnes physiques. Tout comme en cas d'accès, elles ont l'obligation de désigner un consultant en sécurité de l'information et en protection de la vie privée, et un registre des autorisations est tenu par la Commission de la protection de la vie privée, et rendu accessible au public.

De même, le Roi peut déterminer par arrêté royal les cas dans lesquels l'autorisation n'est pas requise, faculté dont il a fait usage, entre autres, dans les cas suivants:

- Arrêté royal du 29 juin 2003 autorisant la Division du Sol de l'Administration de la Gestion de l'Environnement, de la Nature, du Sol et des Eaux du Ministère de la Communauté flamande à utiliser le numéro d'identification du Registre national des personnes physiques
- Arrêté royal du 13 novembre 2002 autorisant la division de l'Emploi - Europe de l'administration de l'Emploi du Ministère de la Communauté flamande à utiliser le numéro d'identification du Registre national des personnes physiques.
- Arrêté royal du 7 juillet 2002 autorisant l'organisme d'intérêt public Enfance et Famille à utiliser le numéro d'identification du Registre national des personnes physiques.
- Arrêté royal du 23 novembre 2001 autorisant l'utilisation du numéro d'identification du Registre national des personnes physiques par l'Agence wallonne pour l'intégration des personnes handicapées.

- Arrêté royal du 15 octobre 2001 autorisant la Sûreté de l'Etat à utiliser le numéro d'identification du Registre national des personnes physiques.
- Arrêté royal du 10 avril 1995 autorisant la gendarmerie à utiliser le numéro d'identification du registre national des personnes physiques.
- Arrêté royal du 30 septembre 1992 autorisant certaines autorités du Ministère de la Région wallonne à utiliser le numéro d'identification du Registre national des personnes physiques.

§ 3. – Le Comité sectoriel du Registre national

Le Comité sectoriel du Registre national, chargé de délivrer les autorisations d'accès au registre et d'utilisation de son numéro, est créé au sein de la Commission de la protection de la vie privée. Composé de trois membres de la CPVP, et de trois membres externes, il a pour tâche, outre l'octroi des autorisations d'accès et d'utilisation du numéro d'identification du Registre national, de veiller au respect de la loi, de formuler toutes les recommandations qu'il jugera utiles au respect de la loi, et d'aider à la solution de tout problème de principe ou de tout litige relatif à l'application de la loi. En outre, la loi lui attribue une compétence d'avis, le comité étant chargé de rendre un avis sur la désignation du consultant en sécurité de l'information et en protection de la vie privée, ainsi qu'au Ministre de l'Intérieur. Enfin, le comité doit veiller au respect des dispositions légales et réglementaires relatives aux documents d'identité, et contrôler la fabrication et la délivrance des cartes électroniques.

Section II. – Jurisprudence de la Commission de la protection de la vie privée relative au numéro d'identification unique en santé

La jurisprudence de la CPVP au sujet de l'utilisation du numéro du registre national ou de celle d'un numéro d'identification spécifique au secteur de la santé, a connu un évolution ces dernières années, évolution qui se clôture par un revirement récent de point de vue.

§ 1er. – De l'utilisation d'un numéro d'identification spécifique au secteur de la santé…

En 2002, la CPVP recommandait d'utiliser un numéro de santé différent du numéro de sécurité sociale et du numéro de registre national, afin d'empêcher la possibilité d'associations de données[323]. Elle se prononçait donc en faveur de l'utilisation d'un numéro de patient unique à l'intérieur du secteur de soins médicaux, numéro qui serait obtenu suite à l'application d'une clé de conversion au numéro de registre national,

[323] Avis n° 14/2002 du 8 avril 2002, et avis n° 19/2002 du 10 juin 2002.

laquelle serait confiée à une organisation intermédiaire chargée d'une mission de gardien lorsque les interconnexions sont nécessaires[324].

En 2004[325], la CPVP poursuivait en se sens, en critiquant le projet d'arrêté royal optant pour la généralisation irréfléchie de l'utilisation du numéro d'identification du registre national, au détriment de la protection de la vie privée des patients vulnérables qui n'ont aucun contrôle sur l'échange des données très sensibles les concernant. Elle recommandait alors l'adoption d'un identificateur unique du patient pour l'échange de données médicales, ainsi que d'assurer l'indépendance de l'organe chargé de l'enregistrement, de mettre au point des normes de sécurité essentielles, et de prévoir le contrôle indépendant sous forme d'un comité sectoriel.

Toujours fidèle à sa conception d'origine, la CPVP déclarait en 2005[326] que le numéro d'identification unique spécifique au secteur de la santé doit être différent du numéro de registre national et du numéro d'identification de sécurité sociale, afin d'empêcher le couplage sans contrôle des données de santé avec d'autres données. Elle précisait que dans les cas où le couplage est quand même souhaité, l'autorisation du comité sectoriel est requise, en tant que garantie du couplage correct utilisant un code d'identification unique pour le patient. Elle apporte toutefois une certaine nuance à sa position, en énonçant que si le projet d'arrêté royal organisant le registre du cancer prévoit que le traitement des données de santé sur lequel se base le RNC s'effectuera au moyen d'un numéro d'identification réservé au traitement des données à caractère personnel dans le domaine de la santé, en attendant l'introduction effective de ce numéro, le numéro d'identification de sécurité sociale – identique à celui du registre national – sera utilisé. La CPVP se montre d'accord avec cette mesure transitoire au motif que le RNC n'est qu'une partie d'un ensemble plus grand, à savoir le traitement des données de santé en général.

§ 2. – … à l'utilisation du numéro d'identification du registre national

Cette nuance apportée à la promotion par la CPVP de la création d'un numéro d'identification spécifique au secteur de la santé était vraisemblablement annonciatrice d'un total revirement de jurisprudence, revirement exprimé en avril 2008 dans son avis relatif au projet de loi portant institution et organisation de la plate-forme eHealth. En effet, ainsi que nous l'avons mentionné ci-dessus, la CPVP s'est prononcée en faveur de l'utilisation du numéro d'identification du registre national dans le cadre des échanges électroniques organisés par eHealth. Il nous semble opportun de reproduire ici un extrait de son avis, au cours duquel elle justifie son changement de vue.

"Il existe plusieurs méthodes pour parvenir à une protection efficace et performante de la vie privée. Grosso modo, on connaît d'une part les méthodes légales (législation et réglementation qui sont imposées par les instruments de droit) et d'autre part, les

[324] Avis n° 30/2002 du 12 août 2002, et avis n° 33/2002 du 22 août 2002.
[325] Avis n°10/2004 du 23 septembre 2004.
[326] Avis n° 01/2005 du 10 janvier 2005.

possibilités techniques (barrières matérielles et technologiques). Un système de protection aura normalement recours à ces deux modes.
45. La question se pose de savoir dans quelle mesure il est ou non utile ou nécessaire d'utiliser une identification sectorielle spécifique (plutôt qu'une identification générale comme le numéro d'identification de la sécurité sociale) lors du traitement de données à caractère personnel relatives à la santé. Une identification sectorielle spécifique consisterait alors en un code ou en un numéro qui serait déduit du numéro d'identification de la sécurité sociale et qui pourrait ou devrait uniquement être utilisé pour certains traitements ou certaines finalités. Cette identification spécifique serait alors le code spécifique pour le secteur "soins de santé", limité ou non aux traitements dans le cadre des prestations curatives, strictement médicales ou élargies à l'ensemble des traitements sur le plan médical et paramédical, ou dans le domaine de la prévention, des mutualités, des obligations de droit social, de l'administration, etc.
46. Il est évident que le choix d'un identifiant sectoriel n'est utile que lorsque les instances qui doivent s'échanger des données à caractère personnel recourent à un même identifiant lors de ces échanges et donc, qu'un même algorithme est utilisé par tous pour déduire l'identifiant sectoriel du numéro d'identification de la sécurité sociale. La définition d'un tel algorithme pourrait être assumée par la plate-forme eHealth en tant qu'élément de son ensemble de tâches. Cette spécialisation de l'identifiant pourrait en outre encore être ventilée par exemple selon le type de prestataire de soins (un médecin généraliste, un hôpital, un laboratoire, une mutualité qui attribue un numéro unique par patient). On peut encore aller plus loin en codant de manière unique chaque prestation et chaque acte médical. Techniquement, tout cela est possible.
47. Il va de soi que la limitation de l'utilisation d'identifiants spécifiques à des secteurs d'application aussi restreints que possible peut rendre le "couplage" de données à caractère personnel plus difficile en dehors de ces secteurs d'application.
48. Il est toutefois tout aussi évident qu'un tel codage doit toujours être suivi d'un déchiffrage ou décodage. Il s'agit en effet (presque) toujours d'un genre de "chaîne" d'informations qui doivent être couplées les unes aux autres pour parvenir à certaines représentations, poser des actes, administrer une médication ou des soins, assurer le suivi et tenir à jour le dossier de suivi administratif. Un problème supplémentaire se pose à cet égard : il peut en effet également arriver que l'on doive pouvoir détecter non seulement la personne, mais aussi parfois certains éléments matériels comme des médicaments ou des prothèses, des implants, etc. Se pose en outre la problématique de la recherche scientifique.
49. Le décodage doit donc pouvoir se faire de manière rapide et sans erreur, et ce sans générer la moindre charge administrative. Dans cette optique, n'appliquer aucun codage (ni décodage) assurerait la plus grande certitude.
50. Le fait de travailler avec une clé d'identification unique constitue le "degré zéro" du codage : le numéro d'identification de la sécurité sociale a justement pour but d'éviter le moindre doute quant à l'identification précise d'une personne. Si notre "nom" était unique, il suffirait en tant qu'identifiant unique. Ce n'est pas le cas (et un numéro standardisé est également plus facile à utiliser dans les TIC).
3.4.3. Analyse et avis de la Commission.
51. Jusqu'à présent, la Commission a déjà souligné à plusieurs reprises la nécessité d'élaborer des numéros d'identification spécifiques à un secteur déterminé. À cet égard,

elle a toujours attiré l'attention sur les dangers éventuels – notamment les couplages effrénés de données à caractère personnel – liés à un numéro d'identification qui est utilisé dans plusieurs secteurs. La Commission rappelle son inquiétude à ce sujet.
52. La Commission prend acte du fait que – contrairement à ce qui se fait dans d'autres États membres de l'Union européenne –, il n'y a pas d'enregistrement central de données dans la plate-forme eHealth. En prenant pour exemple la Banque-carrefour de la sécurité sociale, on a prévu la création d'un répertoire des références qui doit permettre d'afficher à l'écran les données nécessaires par patient et ce, au moyen d'une connexion temporaire avec la base de données où sont enregistrées ces données spécifiques.
53. Un tel système ne permet pas en soi de traiter des données en créant des catégories sur la base du fait que la situation médicale de certaines personnes présente des caractéristiques communes, de rassembler toutes les données de santé relatives à une seule personne, ni d'effectuer des couplages non autorisés de données de santé avec d'autres données à caractère personnel (données sociales, fiscales, familiales, ...).
54. Comme mentionné ci-dessus, le projet opte de facto pour l'utilisation d'une clé d'identification unique générale : le numéro d'identification de la sécurité sociale, le cas échéant le numéro de Registre national.
55. Cette option est également fermement motivée dans l'exposé des motifs du projet : "L'utilisation d'une clé d'identification unique offre des garanties pour une identification correcte des intéressés à chaque stade de l'échange de données à caractère personnel, c'est-à-dire tant pour l'émetteur que pour le destinataire des données à caractère personnel et pour les éventuels autres intervenants."
56. Un numéro d'identification spécifique pour les soins de santé ne sera, de par ce choix, pas appliqué en ce qui concerne l'échange de données à caractère personnel via la plate-forme eHealth.
57. Dans le prolongement de la jurisprudence citée, la Commission a examiné la question de savoir si l'utilisation du numéro d'identification du Registre national ou du numéro d'identification de la sécurité sociale comme identifiant unique au sein de la plate-forme eHealth était recommandée.
58. Vu qu'une identification correcte est d'une importance primordiale d'une part, et qu'au stade actuel des choses, il n'y a pas d'argument suffisant qui s'y oppose d'autre part, il est recommandé de soutenir l'option d'un identifiant fort tel que le numéro d'identification de la sécurité sociale.
59. Un numéro de santé sectoriel général serait utilisé par un nombre si élevé de personnes qu'il n'offrirait peut-être pas une meilleure protection efficace et perceptible de la vie privée. L'utilisation d'un tel numéro sectoriel risque également de devenir une charge organisationnelle importante pour la plate-forme eHealth, ce qui pourrait donner lieu à une identification inefficace.
60. De plus, le développement d'un numéro de santé sectoriel occasionnerait également des problèmes spécifiques. Les méthodes qui entrent en ligne de compte pour l'élaboration d'un tel numéro présentent en effet d'importants inconvénients.
61. Les systèmes suivants sont envisageables en théorie : soit chaque acteur (médecin, hôpital, laboratoire médical, ...) attribue à ses patients un numéro propre (ce qui implique donc qu'un patient recevrait plusieurs numéros), soit chaque patient reçoit un seul numéro de santé et ce, au moyen d'un algorithme appliqué au numéro

d'identification de la sécurité sociale. Les défauts de ces méthodes sont expliqués ci-après.
62. Dans l'hypothèse où un patient recevrait plusieurs numéros spécifiques (chez son médecin traitant, à l'hôpital, ...), il faudrait mettre au point des méthodes permettant aux systèmes informatiques des divers acteurs de toujours pouvoir identifier correctement le patient sur la base de ces différents numéros. Pour ce faire, deux solutions sont possibles :

- *soit un logiciel spécial, conçu par eHealth et chargé des conversions nécessaires, est installé chez chaque acteur. Ceci impliquerait évidemment un défi organisationnel difficilement réalisable ;*

- *soit les conversions sont effectuées par la plate-forme eHealth, ce qui conduirait inévitablement à la constitution d'un monopole au profit de cette instance – ce qui n'est pas souhaité par le projet de loi.*

63. L'hypothèse où chaque patient recevrait un seul numéro d'identification, spécifique au secteur de la santé mais utilisé par chacun au sein de ce secteur et créé par l'application d'un algorithme au numéro d'identification de la sécurité sociale, implique que cet algorithme doive être utilisé par tous les établissements de soins et tous les prestataires de soins. La Commission est consciente du fait qu'en pareil cas, la déduction du numéro d'identification spécifique au secteur de la santé est généralement possible et que l'utilisation d'un tel numéro spécifique offre à peine une protection supérieure contre un couplage illégitime de données à caractère personnel. Cette protection supplémentaire minimale ne compense donc pas le coût plus élevé et le risque d'erreurs lors de l'échange de données à caractère personnel lorsque celui-ci est permis.
64. La Commission conclut que compte tenu de tous les facteurs susmentionnés, l'instauration d'un numéro de santé sectoriel n'est pas l'instrument le plus recommandé pour garantir la protection de la vie privée. Selon la Commission, l'application d'autres techniques de protection de la vie privée, comme la création d'un système dans lequel les données ne font pas l'objet d'un enregistrement centralisé et l'exigence d'une autorisation par le comité sectoriel en combinaison avec la désignation d'un médecin contrôleur et d'un conseiller en sécurité de l'information, doit suffire pour pouvoir empêcher des couplages non souhaités et interdits de différents fichiers de données via la plate-forme eHealth.
65. La Commission émet donc un avis favorable pour l'utilisation du numéro de Registre national et l'accès aux données qui sont demandés"[327].

[327] Avis 14/2008, pp. 13-17, n° 44 à 65.

Section III. – Le cas de la Fondation Registre du Cancer

§ 1er. – L'accès au registre national et l'usage du numéro d'identification du registre national par l'œuvre belge du cancer

En 1989, la CPVP (à l'époque Commission consultative de la protection de la vie privée) s'est prononcée sur la demande de l'œuvre belge du cancer (OBC) à obtenir accès au registre national et à être autorisée à faire usage du numéro d'identification du registre national, en application des articles 5, al. 2 et 8 de la loi du 8 août 1983 organisant un registre national des personnes physiques[328]. Cette demande concernait uniquement l'OBC et son organisation subsidiaire, le Registre National du Cancer (RNC), désireux de pouvoir faire appel à d'autres sources d'information que les mutualités, comme par exemples les laboratoires, les médecins, ou les centres de dépistage. La CPVP estima que, étant donné que l'OBC et le RNC remplissaient des missions d'intérêt général, l'accès au registre national était nécessaire pour éviter les doubles enregistrements, ainsi que pour corriger les données erronées. Pour ce faire, le numéro du registre national subirait un cryptage, autrement dit, il serait rendu illisible l'aide de programmes informatiques. La CCPVP soumit toutefois cette solution à certaines conditions la première tenant à la limitation de l'accès et de l'autorisation, lesquels furent uniquement accordés à l'OBC pour les besoins du RNC. L'usage du numéro fut également réservé aux membres du personnel désignés à cet effet nommément et par écrit par les organes responsables de l'OBC en raison de leurs fonctions et dans les limites de leurs compétences spécifiques. En outre, les données et le numéro d'identification du registre national ne pouvaient être utilisés qu'à des fins d'identifications: aucun accès ne pouvait être accordé pour des données qui n'y contribuaient pas. Enfin, le numéro d'identification du registre national ne pouvait pas être utilisé dans les relations avec les tiers.

§ 2. – Le système du Registre National du Cancer : deux clés de codage

Jusqu'en 2005, l'institution aujourd'hui dénommée Fondation Registre du Cancer (FRC) existait sous le nom et le statut de Registre National du Cancer. Celui-ci utilisait deux types d'informations, à savoir celles permettant d'identifier un cas de manière unique pour obtenir des informations supplémentaires, d'une part, et les données servant de matériel de base aux analyses et notamment à la recherche épidémiologique, d'autre part. S'agissant des premières, un algorithme de hashing était appliqué à différentes données d'identification, à savoir le nom, la date de naissance et le sexe, et ce afin d'aboutir à un résultat unique de 25 caractères. Les autres données transmises au RNC étaient accompagnées de cet identifiant.

La CPVP, estimant que cet algorithme de hashing ne garantissait l'anonymat que dans un sens, a proposé en 1997 d'introduire une deuxième clé réversible au niveau du

[328] Avis n° 89/081 du 10 juillet 1989.

RNC, pour coder les identifiants obtenus par application de l'algorithme[329]. En effet, s'il était impossible de retrouver l'identité de la personne concernée à partir de l'identifiant de 25 caractères, une personne ayant connaissance de l'algorithme pouvait l'appliquer à une personne de sa connaissance et regarder si les 25 caractères obtenus figuraient dans le registre. Avec l'introduction de la deuxième clé de codage, cette dérive était rendue impossible. Dans ce même avis, la CPVP a suggéré que les recherches effectuées sur base des données extraites du RNC reçoivent un avis favorable d'un comité éthique, chargé de vérifier la conformité de la finalité du traitement des données aux buts du RNC, la pertinence des données et l'absence d'atteinte disproportionnée à la vie privée.

Selon la CPVP, le traitement des données effectuées par le RNC pouvait être considéré comme n'entrant pas dans le champ d'application de la loi de 1992 relative à la protection de la vie privée, moyennant le respect de deux conditions. Elle exigeait de la sorte non seulement l'application d'une deuxième clé au niveau du RNC, après application de la première clé (algorithme de hashing) par l'informateur, mais en outre l'exclusion du mois dans les données permettant de déterminer l'âge, celles-ci se limitant à l'année de naissance, la même exigence valant pour l'année de décès. En effet, en possession de la date de naissance complète, du code postal et du sexe, le risque est grand de parvenir à identifier la personne concernée. Mais selon la CPVP, si ces conditions étaient respectées, les données du RNC ne permettaient pas d'identifier les personnes cancéreuses, et ne pouvaient donc être qualifiées de données à caractère personnel, ce qui les exclut du champ d'application de la loi de 1992. En conséquence, le RNC n'était pas soumis à l'obligation de déclaration du traitement de données, si les conditions énoncées ci-dessus étaient respectées.

Par contre, la loi s'applique aux informateurs quant **au traitement en amont** des données, visant à recenser les cas pertinents et à extraire les informations intéressantes. Il s'agit en effet d'un véritable traitement de données à caractère personnel pour communiquer les données au RNC, même si les données transmises sont anonymisées. Les informateurs sont donc tenus de déclarer le traitement de ces données.

Mentionnons enfin que la CPVP estimait qu'à ce sujet, le cadre juridique de la loi de 92 n'est pas adéquat, et réclamait une réponse normative aux problèmes pratiques qu'il pose, concernant entre autres l'obligation d'information de la personne concernée, l'obtention de son consentement, ou encore l'absence d'autorisation légale dans les cas où la loi de 92 le requiert.

§ 3. – Le système actuel de la Fondation Registre du Cancer

Suite aux inconvénients générés par le système de l'algorithme du RNC, la FRC travaille actuellement avec le NISS. En effet, l'application de l'algorithme générait des doublons, auxquels s'ajoutaient parfois des erreurs de données. La recherche des doublons entrainait une perte de temps, et les problèmes étaient souvent impossibles à élucider. La loi du 13 décembre 2006 portant dispositions diverses a pris en compte cette réalité, et autorise, en son article 39, la FRC à utiliser le NISS, reconnaissant la nécessité d'un identifiant valable pour éviter les doublons, ainsi que le besoin de données sûres

[329] Avis de la Commission de la protection de la vie privée concernant le réseau registre national du cancer, avis n° 04/97 du 19 février 1997, http://www.privacycommission.be.

pour être en mesure de les coupler avec des données de morbidité, de mortalité, etc. La volonté politique était donc de travailler sur base de données sûres.

La FRC utilise donc le NISS non-codé, cet usage étant toutefois limité à la mission de la FRC. En outre, le NISS ne peut être communiqué, et l'accès est limité à certaines personnes, qui doivent signer une clause de confidentialité. De plus, aucune recherche du nom ne s'effectue sur base du NISS, et les données sont protégées par différents systèmes. Enfin, les chercheurs n'ont pas accès au NISS, mais uniquement à la banque de données brute où le NISS n'apparaît pas.

Bibliographie

I. Législation, travaux parlementaires et avis

- L. du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, art. 8, § 1er, 2°, *M.B.,* 22 février 1990, www.moniteur.be.
- Question n° 3-3666 de Mme Annemie VAN DE CASTEELE du 28 octobre 2005 (N), *Bull.Q. R.,* Sén., sess. ord. 2005-2006, n° 3-53, http://www.senat.be.
- Réponse du Ministre des Affaires sociales et de Santé publique du 8 novembre 2005, à la question n° 489 de M. Guy D'HAESELEER, du 14 juin 2005 (N), *Bull. Q. R.,* Ch. repr., sess. ord. 2005-2006, n° 099, pp.18006-18010, www.lachambre.be.
- Proposition de résolution visant à soutenir les facteurs critiques de succès nécessaires à la réussite de l'e-société, amendement n°19 proposé par M. Van Nieuwkerke et Mme Zriten le 20 février 2006, *Doc. Parl.,* Ch. repr., sess. ord., 2005-2006, www.lachambre.be.
- L. du 27 décembre 2006 portant dispositions diverses (I), *M.B.,* 28 décembre 2006, art. 4, http://www.moniteur.be.
- Avis de la Commission de la protection de la vie privée n° 14/2008 du 2 avril 2008, à la demande de la Ministre des Affaires sociales et de la Santé publique et de la Ministre de la Fonction publique et des Entreprises publiques concernant un projet de loi portant institution et organisation de la plate-forme eHealth (A/2008/016), http://www.privacycommission.be/fr/docs/Commission/2008/avis_14_2008.pdf.
- Avis du Conseil d'Etat n° 44.351/1/2/3/4, joint au projet de loi portant dispositions diverses (I), déposé à la Chambre des Représentants le 29 mai 2008, Doc. 52 1200/001, http://www.lachambre.be/FLWB/PDF/52/1200/52K1200001.pdf.
- Projet de loi portant dispositions diverses (I), déposé à la Chambre des Représentants le 29 mai 2008, Doc. n° 52 1200/001, http://www.lachambre.be/FLWB/PDF/52/1200/52K1200001.pdf.
- Projet de loi relative à l'institution et à l'organisation de la plate-forme eHealth, déposé à la Chambre des Représentants le 17 juin 2008, Doc. n° Doc 52 1257/001, http://www.lachambre.be/FLWB/PDF/52/1257/52K1257001.pdf.
- Amendements n° 1-12 déposé par M. Goutry et consorts, Chambre des Représentants, 1er juillet 2008, doc n° 52-1257/002, www.lachambre.be/FLWB/pdf/52/1257/52K1257002.pdf.
- Rapport fait au nom de la Commission de la Santé publique, de l'Environnement et du Renouveau de la Société, par M. Detiège, Chambre des Représentants, 9 juillet 2008, Doc. n° 52-1257/003, pp. 35-36, http://www.lachambre.be/FLWB/pdf/52/1257/52K1257003.pdf.
- Comte rendu analytique de la séance plénière de la Chambre des Représentants du 10 juillet 2008, Doc. n° 0050, p. 47, http://www.lachambre.be/doc/PCRA/pdf/52/ap050.pdf.

- Rapport fait au nom de la Commission des Affaires sociales par M. Brotchi, Sénat, Doc. n° 4-863/2, file:///D:/Documents%20and%20Settings/fcols/My%20Documents/HIS%20II/Be-Health/projet%20loi%20mai%202008/rapport%20commission%20affaires%20sociales%20S%C3%A9nat.htm.

II. Doctrine et presse

- Centre de presse international relatif au Conseil des Ministres du 23 décembre 2004, http://www.belgium.be/eportal/application?languageParameter=fr&pageid=contentPage&docId=37478.
- Communiqué du Conseil des Ministres du 7 mars 2008, http://socialsecurity.fgov.be/fr/nieuws_publicaties/nieuwsoverzicht/2008/03.htm#35222; ou www.stomie.be/fra/acc_actu.php?art=1411.
- Journal du Médecin n° 1925 du 10 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1925/9b9ab90e-d0b8-4262-8f11-8a267d972810.vak.html
- Journal du Médecin n° 1926 du 13 juin 2008, http://fr.medisurf.be/protected/publications/artsen-krant/1926/e401f35f-6bec-4f0f-811c-2cf3c69edc72.vak.html.
- Journal du Médecin TV, 15 juillet 2008, http://fr.medisurf.be/protected/archives/WebTV/Archief/20080715.html.
- Le Journal du Médecin n° 1932 du 25 juillet 2008, p. 1, http://www.magazines.medisurf.be/AK1932/akmagazine.aspx?language=fr.
- DECHAMPS, F.R., "Frank Robben. De knowhow van de sociale sector ten dienste van de volksgezondheid", *Citizene*, februari-maart, nummer 01 2008.

Service public fédéral
Sécurité sociale

POLITIQUE SCIENTIFIQUE FEDERALE

Met het oog op het verwerven van een beter inzicht in de gezondheid van de Belgische bevolking, heeft de FOD Sociale Zekerheid het AGORA-project BeLHIS opgestart. Het project is gericht op het beschrijven van methodes om de dynamiek van het sociaal gezondheidssysteem in kaart te brengen (longitudinale benaderingen van de gezondheid). Het stelt een strategie voor om een prospectieve opvolging van de gezondheid van de Belgische bevolking te realiseren. Deze houdt rekening met de Belgische context en de interactie met bestaande initiatieven. Het project BeLHIS wil aan de betrokkenen een referentiekader aanbieden voor de ontwikkeling van een nationaal longitudinaal gezondheidsinformatiesysteem. Dit rapport maakt deel uit van een reeks working papers in het kader van BeLHIS.

Le Service Public Fédéral Sécurité Sociale, à travers un projet AGORA, souhaite enrichir sa connaissance de la santé de la population. Pour ce faire, il a chargé le projet BeLHIS de décrire les méthodologies relatives aux dynamiques sociosanitaires (approches longitudinales de santé) et de proposer des stratégies adaptées au contexte belge, permettant l'interaction et la coordination des différentes initiatives de suivi prospectif de santé. Le projet BeLHIS propose aux institutions et acteurs concernés un cadre de référence afin d'organiser la composante longitudinale du système national d'information sanitaire. Ce rapport fait partie d'un ensemble de « working papers », chacun documentant des aspects particuliers de la recherche du projet BeLHIS.

AGORA Contrat n° AG/JJ/139

UCL Université catholique de Louvain

ULB

Vrije Universiteit Brussel