La loi dite "vie privée" du 8 décembre 1992

Van Gyseghem, Jean-Marc

Published in:
Droits de la personnalité

Publication date:
2013

Document Version
le PDF de l'éditeur

La loi dite « vie privée » du 8 décembre 1992 : la transversalité en évolution

Jean-Marc Van Gyseghem[1]
Directeur de l'Unité de recherche « Libertés et société de l'information » du Centre de Recherche Information, Droit et Société (CRIDS – Université de Namur)
Avocat au barreau de Bruxelles

« Il faut se réserver une arrière-boutique toute nôtre, toute franche, en laquelle nous établissons notre vraie liberté et principale retraite et solitude » (Montaigne)

Introduction

1. La protection des données est considérée comme fondamentale pour le développement de l'individu dans une société démocratique et pour la construction de son bien-être. Elle est au service de l'Homme.

L'on doit également relever que cette protection s'étend aussi à la vie professionnelle de l'individu, qui mérite d'être protégé sur son lieu de travail. Ainsi, la Cour européenne des droits de l'homme a, à maintes reprises, réaffirmé que l'article 8 de la Convention européenne des droits de l'homme : « peut s'étendre à des activités professionnelles ou commerciales »[2]. Cet aspect de surveillance des travailleurs au travail fait l'objet d'une autre contribution dans le présent ouvrage[3].

Si la protection des données est souvent liée à la protection de la vie privée, son champ d'application est beaucoup plus vaste que cela. En effet, plusieurs droits fondamentaux sont concernés. Pensons à la liberté d'expression, à la liberté d'association.

---

[1] Le présent article ne reflète que les opinions personnelles de l'auteur. Il remercie cependant les membres du CRIDS, et tout particulièrement la professeure Cécile de Terwangne et Jean Herveg, assistant-chercheur senior, pour les discussions fructueuses relatives à la protection des données à caractère personnel.

[2] Cour eur. D.H., 28 janvier 2003 (affaire *Peck c. Royaume-Uni*, requête n° 44647/98) ; voy. aussi Cour eur. D.H., 16 février 2000, *Amann c. Suisse*, § 65 ; Cour eur. D.H., 16 décembre 1992, *Niemietz c. Allemagne*, § 29 ; Cour eur. D.H., 25 juin 1997, *Halford c. Royaume-Uni*, §§ 42-46.

[3] F. Omrani, « La vie privée du travailleur : questions choisies, regard critique », cet ouvrage, p. 99.

De manière assez récente, la Charte des droits fondamentaux de l'Union européenne[4] a élevé la protection des données à caractère personnel au rang de droit fondamental, *in se* même s'il garde cette particularité de rester lier à d'autres.

Par ailleurs, une telle protection permet également d'éviter les discriminations entre individus fondées, entre autres, sur les croyances religieuses, les appartenances syndicales, le sexe, la race et les données relatives à la santé.

2. Outre ces considérations basées sur les droits de l'Homme fondamentaux eux-mêmes, l'on doit constater une réelle explosion des technologies de la communication et de l'information pouvant porter atteinte à ce droit à la protection des données à caractère personnel. Ces technologies sont présentes tant dans les activités commerciales que publiques avec l'émergence du concept de gouvernement électronique (eGov).

Le développement de ces technologies implique la prolifération de bases de données informatiques servant d'endroit de stockage et de traitement de nombreuses données à caractère personnel. Ensuite, l'interconnexion de ces bases de données peut dévier vers une traçabilité de l'individu dans ses diverses activités, qu'elles soient privées ou professionnelles.

3. Nous constatons dès lors que les technologies de la communication et de l'information prennent de plus en plus d'importance dans les prises de décision concernant des individus. Nombre de décisions reposent ainsi sur des informations contenues dans ces bases de données.

Il faut donc éviter de voir les avantages de l'utilisation des technologies de l'information et de la communication affaiblir la protection des données à caractère personnel.

Cela implique que les informations doivent être non seulement correctes, mais aussi pertinentes par rapport à l'objectif déterminé et déclaré du traitement. Il faut mettre en œuvre le principe selon lequel on ne peut collecter et traiter que les données à caractère personnel nécessaires à cette finalité. Par conséquent, le responsable de traitement (c'est-à-dire la personne qui va déterminer le but du traitement et les moyens qui vont être mis en œuvre) a une obligation de mise à jour des données et de limitation dans la collecte et le traitement.

4. Par ailleurs, il doit veiller à ce que ces données ne soient pas divulguées sans autorisation de la personne concernée ou sans disposition légale. Cela impose donc la mise en place de mesures organisationnelles et techniques assurant la sécurité du traitement impliquant, entre autres, la collecte et le stockage des données à caractère personnel.

[4] Voy. article 8 de la Charte des droits fondamentaux de l'Union européenne, www.europarl.europa.eu/charter/pdf/text_fr.pdf.

Cette obligation de sécurité implique une responsabilisation du responsable (principe d'*accountability*) renforcée en fonction des données traitées. Il existe, en effet, des données qui sont moins sensibles que d'autres et qui demandent donc une protection éventuellement moindre. À titre d'exemple, nous pouvons donner l'hypothèse d'une base de données ne contenant que des noms et prénoms. Cette base de données contient des données à caractère personnel qui ne sont, normalement, pas sensibles et qui donc génèrent moins de risques et qui, en conséquence, requièrent une sécurité moins perfectionnée. Par contre, ce sera le contraire pour une base de données contenant, par exemple, des données à caractère personnel relatives à la santé.

Nous constatons ainsi qu'il existe deux catégories de données qui peuvent être référencées. Il y a, d'une part, les données sensibles qui sont celles qui touchent l'individu dans ce qu'il a de plus précieux en termes de sphères privées et, d'autre part, les autres données. La première catégorie concerne des données à caractère personnel révélant, par exemple, l'appartenance religieuse, les origines ethniques, ou l'état de santé. Cela peut également être les données génétiques qui ont cette particularité de concerner un grand nombre de personnes, étant celles d'une même fratrie.

5. Parallèlement à cela, il faut nécessairement donner à la personne concernée les moyens de contrôle sur le responsable via un droit d'accès duquel découlera, entre autres, un droit de rectification et d'opposition.

Par ailleurs, on est dans l'obligation de mettre en place un régime de sanction afin de rendre la loi pleinement efficace. En effet, l'on constate qu'une loi sans sanction fait l'objet d'une désobéissance qui la rend parfaitement inefficace.

6. La présente contribution ne se veut pas exhaustive sur le sujet, mais plutôt un point d'entrée dans le monde de la protection des données à caractère personnel via des mots-clefs ou des principes[5].

[5] L'auteur renvoie le lecteur vers la chronique de jurisprudence couvrant les années 2009 à 2011 : « Libertés et société de l'information », *R.D.T.I.*, n° 48 – 3-4/2012, pp. 68 et s., ainsi que « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009.

Section 1
La protection des données à caractère personnel en Europe

§ 1. La Convention européenne des droits de l'homme

7. Au sortir de la Deuxième Guerre mondiale, la nécessité d'avoir un régime de protection des libertés fondamentales mises à mal est devenue criante. Au niveau européen, le Conseil de l'Europe y a répondu par la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH, ci-après) dont le champ d'application est d' « assurer la reconnaissance et l'application universelles et effectives des droits qui y sont énoncés »[6].

8. Parmi les divers droits fondamentaux protégés, nous avons l'article 8 qui concerne la protection de la vie privée et familiale et qui est rédigé comme suit :

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit 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 »[7].

L'on doit relever que « la notion de "vie privée" est une notion large, non susceptible d'une définition exhaustive, qui recouvre l'intégrité physique et morale de la personne (*Pretty c. Royaume-Uni*, n° 2346/02, § 61, CEDH 2002-III, et *Y.F. c. Turquie*, n° 24209/94, § 33, CEDH 2003-IX) »[8], ce qui permet de faire évoluer le concept de concert avec les évolutions de la société tant au niveau philosophique que technique.

La Cour a également rappelé que ce droit à la vie privée est sous-tendu par une large part laissée à l'autonomie de l'individu. Ainsi, dans un arrêt du 11 juillet 2002, elle a rappelé que :

> « la dignité et la liberté de l'homme sont l'essence même de la Convention. Sur le terrain de l'article 8 de la Convention en particulier, où la notion d'autonomie personnelle reflète un principe important qui sous-tend l'interprétation des garanties de cette disposition, la sphère personnelle de chaque individu est protégée, y compris le droit pour chacun d'établir les détails de son identité d'être humain (voir, notamment, Pretty c. Royaume-Uni, n° 2346/02, § 62, CEDH 2002-III, et Mikulić c. Croatie, n° 53176/99, § 53, CEDH 2002-I) »[9].

Par ailleurs, « la garantie offerte par l'article 8 de la Convention est principalement destinée à assurer le développement, sans ingérences extérieures, de la personnalité de chaque individu dans les relations avec ses semblables »[10]. En d'autres termes, « cette disposition protège également le droit à l'identité et au développement personnel ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur »[11].

De plus, ce droit fait partie intégrante de l'individu et il en bénéficie également dans d'autres sphères que celle privée. La Cour européenne des droits de l'homme n'a pas manqué de le rappeler à maintes reprises.

Il en va ainsi dans un arrêt rendu le 28 janvier 2003 qui rappelle que :

> « La "vie privée" est une notion large, qui ne se prête pas à une définition exhaustive. [...]. *Il peut s'étendre à des activités professionnelles ou commerciales.* Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la "vie privée" »[12].

En 2012, elle a également rappelé que « la publication d'une photo interfère dès lors avec la vie privée d'une personne, même si cette personne est une personne publique »[13] et que « dans certaines circonstances, une personne, même connue du public, peut se prévaloir d'une "espérance légitime" de protection et de respect de sa vie privée »[14].

9. Si le principe de l'article 8 consacre le droit à la vie privée et familiale dans le chef de l'individu, il fixe également des exceptions à ce droit au paragraphe 2 ; paragraphe 2 qui « appelle une interprétation étroite »[15]. Cependant,

6 Convention de sauvegarde des droits de l'homme et des libertés fondamentales www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=20/02/20128CL=FRE, 2e considérant.

7 Nous soulignons.

8 Cour eur. D.H., *S. et Marper c. Royaume-Uni* (Requêtes nos 30562/04 et 30566/04), 4 décembre 2008, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052, § 66.

9 Cour eur. D.H., *Cristine Goodwin c. Royaume-Uni* (Requête n° 28957/95), 11 juillet 2002, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=01-65153, § 90.

10 Cour eur. D.H., *von Hannover c. Allemagne* (Requêtes nos 40660/08 et 60641/08), 7 février 2012, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-109027, § 95.

11 Cour eur. D.H., *Peck c. Royaume-Uni* (Requête n° 44647/98), 28 janvier 2003, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-65455 , § 57; nous soulignons.

12 Cour eur. D.H., *Peck c. Royaume-Uni* (Requête n° 44647/98), 28 janvier 2003, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-65455 , § 57; nous soulignons.

13 Cour eur. D.H., *von Hannover c. Allemagne* (Requêtes nos 40660/08 et 60641/08), 7 février 2012, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-109027, § 95.

14 Cour eur. D.H., *von Hannover c. Allemagne* (Requêtes nos 40660/08 et 60641/08), 7 février 2012, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-109027, § 97.

15 Cour eur. D.H., *Rotaru c. Roumanie* (Requête n° 28341/95), 4 mai 2000, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-63075, § 47.

ces exceptions sont entourées par trois notions fondamentales, à savoir celles de nécessité, de texte de loi et de société démocratique.

Dans le cadre de la présente contribution, nous allons nous attarder sur les deux premières dès lors qu'elles sous-tendent également la législation applicable en Belgique en la matière.

Le principe de nécessité ou de proportionnalité impose à chaque état souhaitant limiter le droit à la vie privée de procéder à une analyse de proportionnalité entre, d'une part, la protection de la vie privée et, d'autre part, les intérêts publics. Il s'agit de la pierre angulaire de tout le principe des exceptions de l'article 8 de la Convention.

Cette analyse s'effectuera en choisissant la voie la moins attentatoire à la vie privée pour atteindre l'objectif visé. En d'autres termes, il faudra choisir la mesure la moins invasive en excluant les autres possibilités.

La Cour européenne des droits de l'homme a ainsi considéré « qu'il convenait d'accorder aux autorités nationales compétentes une certaine latitude pour établir un juste équilibre entre les intérêts publics et privés qui se trouvent en concurrence. Cependant, cette marge d'appréciation va de pair avec un contrôle européen (*Funke c. France*, arrêt du 25 février 1993, série A n° 256-A, p. 24, § 55) et son ampleur est fonction de facteurs tels que la nature et l'importance des intérêts en jeu et la gravité de l'ingérence (*Z c. Finlande*, arrêt du 25 février 1997, *Recueil des arrêts et décisions* 1997-I, p. 348, § 99) »[16].

Si le principe de nécessité est contrôlé par la Cour européenne des droits de l'homme, il en va de même pour ce qui concerne l'obligation en vertu de laquelle l'exception doit être prévue par la loi. « Les mots "prévue par la loi" imposent non seulement que la mesure incriminée ait une base en droit interne, mais visent aussi la qualité de la loi en cause : ainsi, celle-ci doit être accessible au justiciable et prévisible »[17]. Cela « implique ainsi – et cela ressort de l'objet et du but de l'article 8 – que le droit interne doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par le paragraphe 1 [...]. Or le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret [...] »[18].

Si les concepts de « base en droit interne » et d'accessibilité ne posent pas de problèmes au niveau de leur compréhension, la Cour a estimé nécessaire de préciser « qu'une norme est "prévisible" lorsqu'elle est rédigée avec assez de

[16] Cour eur. D.H., *Peck c. Royaume-Uni* (Requête n° 44647/98), 28 janvier 2003, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-65455, § 77 ; nous soulignons.

[17] Cour eur. D.H., *Rotaru c. Roumanie* (Requête n° 28341/95), 4 mai 2000, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-63075, § 52.

[18] Cour eur. D.H., *Amann c. Suisse* (Requête n° 27798/95), 16 février 2000, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-62971, § 56.

précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite »[19]. La loi doit donc fixer, entre autres, le genre d'informations pouvant être traitées, les catégories de personnes auprès desquelles les données peuvent être collectées et les circonstances précises dans lesquelles les données peuvent être collectées. Cela permettra donc à l'individu de vérifier la compatibilité de la loi avec la prééminence du droit ainsi qu'un contrôle *a posteriori* de la bonne mise en œuvre de la loi.

La Cour européenne des droits de l'homme a ensuite opéré un lien entre la protection de la vie privée et la protection des données à caractère personnel, entre autres, dans un arrêt du 4 décembre 2008 dans lequel elle précise que :

> « La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article (voir, mutatis mutandis, Z c. Finlande, précité, § 95) ».[20]

§ 2. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

10. En 1981, le Conseil de l'Europe a estimé nécessaire de parvenir à une convention réglant de manière claire la question du traitement des données à caractère personnel même si cette matière faisait déjà l'objet de législations nationales, comme c'était le cas en France.

Le Conseil de l'Europe était arrivé au constat que la protection des données à caractère personnel devait être renforcée compte tenu de « l'utilisation croissante de l'informatique à des fins administratives et de gestion »[21] et du fait qu' « au cours des années à venir, le traitement automatisé des informations continuera à s'imposer dans le domaine administratif et de gestion et cela notamment en raison de l'abaissement des coûts du traitement informatique des données, de l'apparition sur le marché de dispositifs de traitements "intelligents" et de la mise en place de nouveaux équipements de télécommunications pour la transmission des données »[22].

[19] Cour eur. D.H., *Rotaru c. Roumanie* (Requête n° 28341/95), 4 mai 2000, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-63075, § 55.

[20] Cour eur. D.H., *S. et Marper c. Royaume-Uni* (Requêtes n^{os} 30562/04 et 30566/04), 4 décembre 2008, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052, al. 103.

[21] Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, § 1, al. 2, http://conventions.coe.int/Treaty/FR/Reports/Html/108.htm.

[22] Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, § 1, al. 3, http://conventions.coe.int/Treaty/FR/Reports/Html/108.htm.

Il est intéressant d'observer que cette convention a mis en place une protection adaptée aux données à caractère personnel et des concepts toujours actuels même si la convention fait actuellement l'objet d'une révision.

Nous ne nous attarderons guère plus sur cette convention dans le cadre de la présente contribution, non pas qu'elle soit inintéressante – que du contraire –, mais parce que nous analyserons la loi belge qui s'en inspire fortement.

§ 3. La Charte des droits fondamentaux de l'Union européenne

11. Depuis l'entrée en vigueur du Traité de Lisbonne, la Charte des droits fondamentaux de l'Union européenne est juridiquement contraignante.

12. Si l'article 7 de ce texte consacre classiquement la protection du droit au respect de la vie privée, l'article 8 présente l'originalité de garantir – au sein d'un catalogue général de droits fondamentaux – un droit autonome à la protection des données à caractère personnel. Cet article élève ainsi donc la protection des données à caractère personnel au rang de droit fondamental *in se*, même s'il garde cette particularité de rester lier à d'autres tels que la liberté d'association, le droit à la vie privée et la liberté d'expression.

Cet article 8 dispose donc que :

> « 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
>
> 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
>
> 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante »[23].

Il est intéressant de constater que la note du Présidium[24] rattache ce droit tant à l'article 8 de la CEDH qu'à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ratifiée par tous les États membres, ou encore à la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dont il sera question ci-dessous.

[23] http://www.europarl.europa.eu/charter/pdf/text_fr.pdf.

[24] Note du Présidium sur le projet de Charte des droits fondamentaux de l'Union européenne, www.europarl.europa.eu/charter/pdf/04473_fr.pdf, p. 11.

Cette filiation entre ces divers textes de base en matière de protection des données à caractère personnel est établie afin d'en renforcer l'ancrage dans le droit européen d'autant plus que, en vertu de l'article 52.3 de la Charte[25], le sens du droit à la protection des données à caractère personnel ainsi que sa portée sont les mêmes que ceux conférés par la CEDH.

Le Presidium a motivé cela comme suit :

> « Le paragraphe 3 vise à assurer la cohérence nécessaire entre la Charte et la CEDH en posant le principe que, dans la mesure où les droits de la présente Charte correspondent également à des droits garantis par la CEDH, leur sens et leur portée, y compris les limitations admises, sont les mêmes que ceux que prévoit la CEDH. Il en résulte en particulier que le législateur, en fixant des limitations à ces droits, doit respecter les mêmes standards que ceux fixés par le régime détaillé des limitations prévu dans la CEDH, sans que ceci porte atteinte à l'autonomie du droit communautaire et de la Cour de justice des Communautés européennes. La référence à la CEDH vise à la fois la Convention et ses protocoles. Le sens et la portée des droits garantis sont déterminés non seulement par le texte de ces instruments, mais aussi par la jurisprudence de la Cour européenne des droits de l'homme et par la Cour de justice des Communautés européennes. La dernière phrase du paragraphe vise à permettre au droit de l'Union d'assurer une protection plus étendue.
>
> La liste des droits qui peuvent, au stade actuel et sans que cela exclue l'évolution du droit, de la législation et des traités, être considérés comme correspondant à des droits de la CEDH au sens du présent paragraphe est reproduite ci-dessous. Ne sont pas reproduits les droits qui s'ajoutent à ceux de la CEDH »[26].

Cela doit également être lu en parallèle avec l'article 6 du Traité de l'Union qui prescrit que :

> « 1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités.
>
> Les dispositions de la Charte n'étendent en aucune manière les compétences de l'Union telles que définies dans les traités.

[25] Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

[26] Note du Présidium sur le projet de Charte des droits fondamentaux de l'Union européenne, www.europarl.europa.eu/charter/pdf/04473_fr.pdf, p. 48.

Les droits, les libertés et les principes énoncés dans la Charte sont interprétés conformément aux dispositions générales du titre VII de la Charte régissant l'interprétation et l'application de celle-ci et en prenant dûment en considération les explications visées dans la Charte, qui indiquent les sources de ces dispositions.

2. L'Union adhère à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Cette adhésion ne modifie pas les compétences de l'Union telles qu'elles sont définies dans les traités.

3. Les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, font partie du droit de l'Union en tant que principes généraux. »

Pour ce qui est de l'exercice de ce droit, la note du Presidium renvoie à la directive 95/46 et à l'article 52 de la Charte pour ce qui est des limitations possibles.

§ 4. La directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

13. L'Europe s'est dotée, en 1995, d'un texte relatif à la protection des données à caractère personnel sous forme de directive qui est la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (directive 95/46 ci-après).

Cette directive a été transposée en Belgique par la loi du 11 décembre 1998 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Nous ne l'analyserons donc pas plus amplement ici dès lors que nous nous attarderons plus longuement sur la législation belge, objet de la présente contribution.

§ 5. La directive européenne vie privée et communications électroniques

14. Afin de donner un rapide panorama des principaux textes européens en matière de vie privée et de protection des données à caractère personnel sans pour autant les aborder spécifiquement dans la présente contribution, notons la directive 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[27] (directive dite « vie privée et communications électroniques ») qui est une directive spécifique venant compléter la directive générale (95/46/CE) pour réglementer la protection des données dans le secteur spécifique des communications électroniques. Cette directive fait partie du « paquet télécom ».

Cette directive 2002/58 ne s'applique qu'aux fournisseurs de services de communications électroniques accessibles au public, ce qui peut, dans certains domaines, générer des distorsions de concurrence au bénéfice d'opérateurs ne fournissant pas de tels services de communications électroniques accessibles au public, mais offrant cependant des services à valeur ajoutée basés sur la localisation tels que ceux que l'on trouve sur les GPS de voiture.

Ce texte règle aussi le recours aux *cookies* et l'envoi de communications non sollicitées (*spam*).

Cette directive traite de la sécurité en rappelant, conformément à la directive 95/46, que des mesures d'ordre technique et organisationnel doivent être prises. Mais le texte va plus loin sur le plan de la sécurité et impose également une obligation, à charge du fournisseur de services, d'informer les abonnés des risques particuliers de violation de la sécurité du réseau « et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable »[28].

15. La grande nouveauté apportée au texte lors de sa révision fin 2009[29] tient dans l'instauration d'une obligation d'informer l'autorité nationale de contrôle des « violations des données à caractère personnel »[30] : des incidents touchant à la sécurité susceptibles d'entraîner des risques graves pour la vie privée de l'abonné (par exemple, vol ou usurpation d'identité, atteinte à l'intégrité physique, humiliation grave ou réputation entachée). Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel et la vie privée d'un abonné ou d'un particulier, le fournisseur doit aussi avertir de la violation, sans retard, l'abonné ou le particulier concerné, sauf si le fournisseur a prouvé à l'autorité compétente qu'il a mis en œuvre les mesures de protection technologiques appropriées en réponse à cette violation.

16. La confidentialité des communications est également prévue de manière telle que les États membres doivent garantir, « par la législation nationale, la

[27] J.O.U.E., L 201 du 31 juillet 2002, pp. 37-47.

[28] Directive 2002/58/CE, article 4.2.

[29] Directive 2002/58 modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, J.O., L 337 du 18 décembre 2009, p. 11.

[30] Directive 2002/58/CE, article 4.3.

confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes »[31]. Cette confidentialité doit être garantie à l'égard de tout tiers à une communication électronique : il est interdit à toute autre personne que les utilisateurs parties à la communication électronique « d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs [parties à la communication électronique] sauf lorsque cette personne y est légalement autorisée »[32]. Bien entendu, le stockage technique nécessaire à l'acheminement d'une communication n'est pas, lui, interdit[33].

17. Par ailleurs, le stockage des informations ou l'accès à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur « n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement »[34]. La directive met donc en exergue le consentement informé de l'abonné ou de l'utilisateur.

De plus et sauf exception, « les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication » sous réserve d'exceptions prévues par les États membres ou par la directive elle-même[35]. Il est à noter que, parmi ces exceptions, nous retrouvons l'activité commerciale du fournisseur de services qui lui permet de traiter ces données relatives au trafic « pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable »[36], consentement qui peut être retiré à tout moment.

18. La directive traite également des données de localisation autres que les données relatives au trafic en prescrivant que leur traitement ne pourra être effectué « qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée »[37]. Le consentement devra, bien

31 Directive 2002/58/CE, article 5.
32 Directive 2002/58/CE, article 5.1.
33 Directive 2002/58, article 5.1, *in fine*.
34 Directive 2002/58, article 5.3.
35 Directive 2002/58, article 6.1.
36 Directive 2002/58, article 6.3.
37 Directive 2002/58, 9.1.

entendu, être éclairé, ce qui implique une information quant « au type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée »[38]. Par ailleurs et en cas de consentement, les utilisateurs ou les abonnés « doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication »[39].

19. Pour ce qui concerne les communications électroniques non sollicitées, mieux connues sous le vocable de *spam*, elles sont soumises au consentement préalable. Ce consentement est présumé lorsque l'émetteur d'une telle communication « a, dans le cadre d'une vente d'un produit ou d'un service, obtenu directement de ses clients leurs coordonnées électroniques en vue d'un courrier électronique »[40] et « pour autant que lesdits clients se voient donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation des coordonnées électroniques lorsqu'elles sont recueillies et lors de chaque message, au cas où ils n'auraient pas refusé d'emblée une telle exploitation »[41]. L'article 13.4 précise également que « dans tous les cas, il est interdit d'émettre des messages électroniques à des fins de prospection directe en camouflant ou en dissimulant l'identité de l'émetteur au nom duquel la communication est faite, ou sans indiquer d'adresse valable à laquelle le destinataire peut transmettre une demande visant à obtenir que ces communications cessent ».

Il faut relever que cette directive a été transposée en Belgique par la loi du 13 juin 2005 relative aux communications électroniques qui n'est pas l'objet de la présente contribution.

§ 6. La directive sur la rétention des données (*data retention*)

20. Nous devons également mentionner la directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications qui a modifié la directive 2002/58/CE analysée ci-dessus. Cependant, elle fait l'objet d'une procédure de modification suite aux refus de plusieurs États membres de la transposer ou à des décisions de cours constitutionnelles annulant les lois de transposition pour inconstitutionnalité.

38 Directive 2002/58, 9.1.
39 Directive 2002/58, 9.2.
40 Directive 2002/58, 13.2.
41 Directive 2002/58, 13.2.

Il est à noter que la Belgique se trouve dans le premier groupe dès lors qu'elle n'a jamais voté de loi de transposition.

21. Le principe de cette directive qui s'inscrit dans la mouvance des textes pris dans un contexte de lutte contre le terrorisme et la criminalité organisée est d'obliger les fournisseurs de services de communications électroniques accessibles au public à conserver une série de données pour une durée allant de six mois à deux ans.

Ces données sont précisées à l'article 5 de cette directive et sont, par exemple, le numéro d'appel de l'appelant, le numéro IMEI de l'appelé, etc.

Cette directive continue à faire débat par rapport à sa légalité dans nombre d'États membres et a donné lieu à des décisions de plusieurs cours constitutionnelles tel que cela a été le cas en Allemagne.

Nous devons bien avouer que cette directive soulève nombre de questions par rapport à certains principes clés en matière de protection de la vie privée tels que celui de nécessité prévu par l'article 8 de la CEDH.

Section 2
La protection des données à caractère personnel en Belgique

22. La Belgique s'est dotée d'une loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel le 8 décembre 1992 (loi « vie privée », ci-après). Si elle n'était pas précurseur en la matière, elle précédait cependant la directive 95/46/CE. L'adoption de cette directive par l'Europe a entraîné une modification de la loi belge par l'effet de la transposition de la directive. Cela portait, entre autres, sur la modification[42] ou l'introduction[43] de définitions et de concepts. Les champs d'application matériel, personnel et territorial ont également été modifiés tout comme la notion de contrôle des traitements tant interne[44] qu'externe par la Commission de la protection de la vie privée via la déclaration de traitement et des compétences élargies. La question des transferts de données vers des pays tiers reprenant les concepts de la directive 95/46 a également été visée.

Par la suite, la loi a encore fait l'objet de modifications avec l'introduction des comités sectoriels et l'article 34 concernant le budget.

[42] « Maître de fichier » devient « responsable de traitement » et « gestionnaire de fichiers » devient « sous-traitant ».

[43] « Tiers », qui est autre que le responsable de traitement, le sous-traitant ou personnes travaillant sous leur autorité directe et « destinataire », qui peut faire partie de la structure du responsable de traitement ou du sous-traitant (département, administration).

[44] Obligation de sécurité également à charge du sous-traitant et disparition de l'obligation de faire un « état pour chaque traitement » au profit d'une « déclaration » moins précise, mais non moins utile.

23. Il est important de souligner que la loi « vie privée » ne peut pas être lue sans avoir à l'esprit les normes internationales telles que la Convention européenne des droits de l'homme et la directive 95/46.

Ainsi, dans son arrêt du 18 mars 2010, la Cour constitutionnelle a considéré que :

> « [...] La Cour peut examiner si le législateur a respecté les obligations internationales qui découlent des dispositions invoquées de la directive précitée [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 de la convention n° 108 [du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel] auxquelles la loi précitée du 8 décembre 1992 [relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel] et ses modifications ultérieures donnent exécution. Ces obligations forment un *ensemble indissociable* des garanties qui sont reproduites à l'article 22 de la Constitution. »[45]

La Cour réaffirme donc la filiation de l'article 22 de la Constitution et des normes qui lui sont inférieures telle que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel avec les normes internationales qui sous-tendent le droit à la protection de la vie privée. Cela donne également une clef d'analyse dès lors que les interprétations de l'article 8 de la CEDH rendue par la Cour européenne des droits de l'homme de Strasbourg sont applicables. Cela a été confirmé une nouvelle fois, en d'autres termes, par la Cour qui a considéré qu' « il ressort des travaux préparatoires de [l']article [22] que le Constituant [a] cherché à mettre le plus possible la proposition en concordance avec l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH), afin d'éviter toute contestation sur le contenu respectif de l'article de la Constitution et de l'article 8 de la CEDH » (*Doc. parl.*, Chambre, 1993-1994, n° 997/5, p. 2) »[46].

§ 1. Notions de base

A. Données à caractère personnel et personnes concernées

24. La loi « vie privée » définit les données à caractère personnel comme « étant toute information concernant une personne physique identifiée ou

[45] C.C. (29/2010), 18 mars 2010, www.const-court.be; nous soulignons.

[46] C.C. (166/2011), 10 novembre 2011, www.const-court.be, B16.6. Voir également C.C. (122/2011), 7 juillet 2011, www.const-court.be, B. 3.

identifiable, désignée ci-après "personne concernée" ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[47].

La personne concernée sera cette personne physique concernée par les informations.

25. Nous attirons l'attention sur le fait que cette définition ne vise qu'une personne physique à l'exclusion des personnes morales. Cette limitation aux personnes physiques peut s'expliquer par le fait que la loi traite d'un droit fondamental qui, par définition, n'est l'attribut que des dites personnes physiques. Cependant, « quand cependant de telles données reposent sur des données qui à leur tour concernent une personne physique, la [loi "vie privée"] peut s'appliquer »[48].

26. Par ailleurs, la définition est extrêmement large dès lors qu'elle vise toute information sans aucune limitation. L'information peut donc être liée à la sphère privée comme publique.

L'on doit relever que :

> « n'exclut pas l'application de la loi le fait que les données soient relatives à un commerçant, un indépendant, une profession libérale ou l'administrateur d'une société. La loi ne fait pas de distinction entre le caractère public ou privé de la donnée. Le fait qu'elles se trouvent dans des registres publics accessibles au public n'exclut pas non plus son application »[49].

Ces données à caractère personnel peuvent être le nom, le prénom, les adresses IP, un *log* ainsi que l'a considéré la Cour d'appel de Liège dans un arrêt du 22 octobre 2009[50]. Des images vidéo peuvent également être considérées comme des données à caractère personnel[51].

[47] Article 1, § 1, de la loi « vie privée ».

[48] J.-Ph. Moiny et J.-M. Van Gyseghem, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 83 ; voy. également Comm. Courtrai (1re ch.), 19 juin 2003, *T.G.R.-T.W.V.R.*, 2007, liv. 2, p. 100, confirmé par Gent, 6 janvier 2005, *T.G.R.-T.W.V.R.*, liv. 2, 2007, pp. 92-93. La Cour d'appel de Bruxelles a considéré que « le droit au respect de la vie privée bénéficie aussi, dans une certaine mesure, aux personnes morales. Dès lors, il peut être admis que le droit au respect de la vie privée des personnes morales englobe la protection de leurs secrets d'affaires », Bruxelles, 30 juin 2010, *J.L.M.B.*, 25/2011, p. 1184. Il semble cependant que la Cour se soit limitée à l'article 8 de la CEDH et ne soit pas allée jusqu'à la loi « vie privée ».

[49] J.-Ph. Moiny et J.-M. Van Gyseghem, « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T.I.*, 2009, p. 83.

[50] Liège (7e ch.), 22 octobre 2009, *R.D.T.I.*, n° 38/2010, pp. 95 et s.

[51] Voy. Corr. Bruxelles (51e ch.), 14 janvier 2002, *A&M*, 2002, p. 198. Voy. aussi Liège (6e ch.), 27 juin 2003, *R.D.T.I.*, 2004, n° 18, p. 105 et Mons (1re ch.), 2 mai 2005, précité, p. 1057.

Le Conseil d'État a également estimé, dans un arrêt du 27 octobre 2005, qu' « un test d'haleine entraîne la collecte d'une donnée à caractère personnel »[52].

27. Il faut, mais il suffit, par ailleurs que la personne physique soit identifiée ou identifiable. Si le premier terme est assez évident à comprendre, tel n'est pas le cas du second qui donne lieu à beaucoup de discussions. Pour en comprendre la portée, nous devons nous reporter au considérant 26 de la directive 95/46 qui précise que « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne »[53]. Pour considérer qu'une personne soit identifiable, le responsable de traitement devra donc vérifier si lui-même ou toute autre personne peut identifier la personne. Cela rend, bien évidemment, également la définition extrêmement large dès lors que, dès l'instant où quelqu'un pourra identifier la personne concernée, il s'agira d'une donnée à caractère personnel.

Imaginons, par exemple, qu'une société de statistique soit chargée par plusieurs chaînes de supermarché de réaliser une enquête de taux de fréquentation de divers établissements et de voir si les clients sont fidèles à une seule chaîne ou s'ils en fréquentent plusieurs. Pour ce faire, la société de statistique enregistre les plaques d'immatriculation des véhicules entrant dans les parkings des supermarchés pour ensuite analyser leur fréquentation. Au regard de la définition de l'article 1er, § 1 de la loi « vie privée », il s'agit de données à caractère personnel dès lors qu'un tiers peut identifier les propriétaires des véhicules, à savoir la DIV. Or, la société de statistique n'a pas pour objectif de procéder à une telle identification et, de surcroît, n'a pas accès aux registres de la DIV.

Il serait donc utile d'analyser cette définition de manière contextuelle et en rapport avec la finalité du traitement. Cela permettrait de considérer que la société de statistique ne traite pas de données à caractère personnel et ne tomberait donc pas dans le champ d'application matériel de la loi.

Nous observons donc qu'une analyse contextuelle de la loi « vie privée » est nécessaire afin d'éviter de la rendre contre-productive par l'imposition d'obligations dont certaines ne pourraient pas être rencontrées par le responsable de traitements.

B. Responsable de traitement

28. Un responsable de traitement est « la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à

[52] C.E., arrêt n° 150.861 du 27 octobre 2005, http://www.raadvst-consetat.be.

[53] Nous soulignons.

caractère personnel »[54]. La loi précise également que « lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance »[55].

29. Dans le cadre de la présente contribution, seul le premier alinéa nous intéresse dès lors qu'il donne les trois critères permettant de déterminer le responsable de traitement, à savoir la détermination des finalités et des moyens.

Le Groupe de l'article 29 a considéré qu' « être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres »[56]. Il s'agira bien souvent d'une analyse factuelle qui obligera le juge, par exemple, à vérifier si le responsable de traitement peut être considéré comme tel. Le Groupe de l'article 29 ne dit rien d'autre en considérant que la capacité de déterminer « se déduira généralement d'une analyse des éléments factuels ou des circonstances de l'espèce : il conviendra d'examiner les opérations de traitement en question et de comprendre qui les détermine, en répondant dans un premier temps aux questions "pourquoi ce traitement a-t-il lieu ?" et "qui l'a entrepris ?" »[57].

30. Outre cette capacité de déterminer, il faut qu'il y ait détermination des finalités et des moyens.

Selon le Groupe de l'article 29 :

> « On peut en outre affirmer que la détermination des finalités et des moyens revient à établir respectivement le "pourquoi" et le "comment" de certaines activités de traitement. Dans cette optique, et puisque ces deux éléments sont indissociables, il est nécessaire de donner des indications sur le degré d'influence qu'une entité doit avoir sur le "pourquoi" et le "comment" pour être qualifiée de responsable du traitement.
>
> [...]
>
> Lorsqu'il s'agit d'évaluer la détermination des finalités et des moyens en vue d'attribuer le rôle de responsable du traitement, la question centrale qui se pose est donc le degré de précision auquel une personne doit déterminer les finalités et les moyens afin d'être considérée comme un

[54] Article 1, § 4, al. 1, de la loi « vie privée ».

[55] Article 1, § 4, al. 2, de la loi « vie privée ».

[56] Groupe de l'article 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.

[57] Groupe de l'article 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 9.

> responsable du traitement et, en corollaire, la marge de manœuvre que la directive laisse à un sous-traitant. Ces définitions prennent tout leur sens lorsque divers acteurs interviennent dans le traitement de données à caractère personnel et qu'il est nécessaire de déterminer lesquels d'entre eux sont responsables du traitement (seuls ou conjointement avec d'autres) et lesquels sont à considérer comme des sous-traitants, le cas échéant »[58].

Par finalité, l'on entend l'objectif poursuivi par le responsable de traitement, le « pourquoi » évoqué par le Groupe de l'article 29.

Les moyens, pour leur part, expriment la façon par laquelle on atteindra l'objectif, la finalité et pourront être techniques, mais aussi organisationnels.

Au terme d'une telle analyse, la Cour d'appel de Mons a considéré qu'un détective privé devait être qualifié de responsable de traitement au motif qu'il a établi un rapport contenant des données à caractère personnel en utilisant un logiciel de traitement de texte[59]. Cette analyse est cependant contestable dès lors qu'un détective pourrait être considéré comme agissant pour le compte d'un tiers et sous ses instructions, ce qui constitue les attributs d'un sous-traitant ainsi que nous le verrons ci-dessous.

À noter que cette qualité de responsable de traitement peut être partagée.

C. Sous-traitant

31. Le sous-traitant est défini comme étant « la personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données »[60].

Il ressort de cette définition que, pour être considéré comme sous-traitant, l'on ne peut pas être dans une relation hiérarchique avec le responsable de traitement et que l'on doit traiter des données à caractère personnel pour son compte. Bien souvent, le sous-traitant interviendra sur les moyens mis en œuvre pour atteindre les finalités dès lors qu'il sera fait appel à lui pour ses compétences particulières. Ce sera le cas de fournisseurs de service internet tels que les fournisseurs de *cloud computing*[61].

[58] Groupe de l'article 29, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », WP 169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 14.

[59] Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, pp. 80 et s.

[60] Article 1, § 5, de la loi « vie privée ».

[61] Voy. à ce propos, J.-M. Van Gyseghem, « *Cloud computing* et protection des données à caractère personnel : mise en ménage possible ? », *R.D.T.I.*, issue 42, pp. 35-50. Voy. également Groupe de l'article 29, « Avis 05/2012 sur l'informatique en nuage », http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf.

D. Traitement

32. Par traitement, l'on doit entendre « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel »[62].

Le traitement est donc un ensemble d'opérations extrêmement large.

Le fait de collecter ou de consulter des données à caractère personnel est déjà considéré comme un traitement de données à caractère personnel. Il en va de même lorsqu'un logiciel de traitement de texte[63] est utilisé pour enregistrer des données à caractère personnel.

La Cour d'appel de Mons, dans l'arrêt déjà cité ci-dessus, a ainsi considéré que :

> « le rapport d'un détective privé constitue en effet un traitement de données à caractère personnel au sens de la loi du 8 décembre 1992 lorsque, comme en l'espèce, il contient [des données à caractère personnel], à savoir toute information se rapportant à une personne physique identifiée ou identifiable, lorsque ces données ont subi un "traitement automatisé", à savoir tout traitement dans lequel le(s) technologie(s) de l'information (et de la communication) intervien(nen)t, tel que le traitement de texte utilisé en informatique »[64].

Dans un arrêt du 19 novembre 2009, la Cour d'appel de Liège a considéré, pour sa part, que le fait, pour un gestionnaire de site internet, d'enregistrer et de conserver des données pour lui permettre d'envoyer des courriels non sollicités constitue un traitement de données à caractère personnel[65].

33. Il est également utile de rappeler que la notion de traitement ne s'applique pas uniquement lors d'opérations à l'aide de procédés automatisés, mais également à des traitements manuels. En effet, la loi « vie privée » « s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie,

[62] Article 1, § 2; Voy. également, sur cette notion, Cass., 16 mai 1997, *J.T.*, 1997, p. 779; Anvers, 27 septembre 1995, *A.J.T.*, 1995-96, note J. Dumortier; Th. Léonard, « La protection des données à caractère personnel et l'entreprise », *in Guide juridique de l'entreprise*, 2e éd., Titre XI, Livre 112, Diegem, Kluwer, 1996, p. 15, n° 130; en France, voy. notamment : Cass. (ch. crim.), 3 novembre 1987, *D.*, 1988, J, pp. 17 et s., note H. Maisl; T.G.I. Créteil, 10 juillet 1987, *D.*, 1988, J., pp. 319 et s., note J. Frayssinet; J. Frayssinet, « La Cour de cassation et la loi informatique, fichiers et libertés ou comment amputer une loi tout en raffermissant son application », *J.C.P.*, 1988, I, n° 3223; *Idem*, « Contre l'excessive distinction entre fichier et dossier : Le pas en avant du tribunal correctionnel de Paris », *Expertises*, 1990, pp. 16 et s.

[63] Voy. *supra*, p. 26, n° 30

[64] Mons (14e ch.), 2 mars 2010, *R.D.T.I.*, n° 41/2010, p. 83 avec la note de F. Dumortier.

[65] Liège (7e ch.), 19 novembre 2009, *DAOR*, 2010/96, p. 453.

ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »[66]. Par fichier, l'on entend « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique »[67]. En clair, pour que la loi s'applique également à un traitement effectué par des moyens non automatisés, « il faut des données ordonnées et que celles-ci soient accessibles en fonction de critères déterminés. À cet égard, l'ordre et la méthode conduisent inévitablement à l'application de la loi »[68]. Un classement sur base des noms des personnes, par ordre alphabétique, constitue un fichier au sens de la loi « vie privée ».

§ 2. Principes de la loi « vie privée »

A. Transparence

34. L'un des principes fondamentaux de la loi « vie privée » est la notion de transparence de tout traitement à l'égard de la personne concernée. Cette transparence est, évidemment, tempérée par le devoir de confidentialité à l'égard des tiers.

35. Ce principe se retrouve à divers niveaux dans la loi à commencer par l'obligation d'informer la personne concernée tel que cela figure à l'article 9. Ainsi, le responsable de traitement « doit fournir à la personne concernée auprès de laquelle il obtient les données la concernant et au plus tard au moment où ces données sont obtenues » ou « si elles n'ont pas été obtenues auprès de la personne concernée, le responsable du traitement ou son représentant doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données » au moins une série d'information étant, entre autres, l'identité du responsable de traitement, les finalités du traitement, les droits de la personne concernée, etc.

Pour certaines données telles que celles relatives à la santé ou 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, des informations complémentaires doivent être données ainsi que cela est prévu au chapitre III de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992

[66] Article 3, § 1er, de la loi « vie privée ».

[67] Article 1, § 3, de la loi « vie privée ».

[68] C. de Terwangne, J. Herveg, J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication : introduction à la protection des données dans la preuve des causes de divorce*, Kluwer, 2005, p.

relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (arrêté royal, ci-dessous).

Cette obligation d'information connaît cependant certaines exceptions :

> « a) lorsque, en particulier pour un traitement 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, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ;
>
> b) 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 »[69].

La première exception est, en réalité, une obligation d'information différée dès lors que l'arrêté royal prévoit que le responsable de traitement « communique cette information, à la première prise de contact, avec la personne concernée »[70]. Cela est justifié par le fait que cette exception se base sur une impossibilité ou une disproportion de moyens à mettre en œuvre pour remplir l'obligation d'information. Cela implique donc que, dès l'instant où un tel obstacle disparaît, l'obligation doit être respectée.

À cela s'ajoutent des exceptions propres à certaines activités telles que le journalisme[71], la Sûreté de l'État, le Service général du renseignement et de la sécurité des forces armées, etc.

36. Un autre aspect de la loi découlant de ce principe de transparence est l'obligation de déclarer le traitement à la Commission de la protection de la vie privée préalablement à sa mise en œuvre tel que cela est prévu à l'article 17 de la loi.

Cette déclaration ne connaît que quelques exceptions prévues par l'arrêté royal en ses articles 51 et suivant ainsi que pour ce qui concerne les traitements manuels et sur microfiches[72]. À noter que les avocats sont soumis à la loi et à cette obligation de déclaration[73].

Si cette étape peut paraître fastidieuse à certains, et surtout à certaines entreprises, elle n'en demeure pas moins importante pour, au moins, trois raisons :

- Porter l'existence du traitement à la connaissance du public via le registre public accessible sur le site internet de la Commission de la protection de

[69] Article 9, § 2, de la loi « vie privée ».

[70] Article 30, de l'arrêté royal.

[71] Article 3, § 3, de la loi « vie privée ».

[72] Article 17, § 1er, de la loi « vie privée ».

[73] Voy. C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, 2005, pp. 149 et s.

la vie privée. Cela permet également à la personne concernée potentielle d'appréhender ledit traitement à l'instar de ce qu'elle ferait avec une loi. Cela lui permet donc de pouvoir évaluer la portée d'un traitement, les mesures de sécurité qui l'entourent, etc. L'attention est cependant attirée sur le fait que la déclaration ne dispense pas le responsable de traitement de fournir une information à la personne concernée.

- Obliger le responsable de traitement à analyser son traitement en termes de finalités, de qualité des données, de sécurité, etc. Cela n'est pas négligeable, et ce, surtout pour de petites structures qui n'ont pas nécessairement un service juridique ou un délégué à la protection des données en son sein. Une telle analyse peut donc se révéler utile pour éviter que la protection des données à caractère personnel ne soit négligée par manque de temps ou de ressources.
- Permettre à la Commission de la protection de la vie privée d'opérer un contrôle et le cas échéant d'interroger le responsable de traitement sur certaines ambiguïtés de sa déclaration. À condition, évidemment, qu'elle en ait les capacités logistiques et financières…

Il est utile de rappeler que l'arrêté royal prévoit certaines exemptions de déclaration qui sont limitées et à interpréter limitativement tel que prévu aux articles 51 et suivants.

À noter également que certains traitements requièrent une autorisation préalable délivrée par les comités sectoriels. Il en va ainsi pour le transfert de données à caractère personnel relatives à la santé, du numéro de registre national[74], etc.

37. Ce principe de transparence donne également naissance aux droits des personnes concernées avec, en premier lieu, celui d'accès.

Le droit d'accès est fondamental pour la personne concernée afin qu'elle puisse procéder à diverses vérifications dont, bien évidemment, celle de savoir si des données à caractère personnel la concernant sont traitées. Si la réponse est positive, elle pourra alors prendre connaissance des données traitées et s'assurer que le traitement est conforme à la loi « vie privée ».

De ce premier droit qui est, en quelque sorte, une porte d'entrée au traitement pour la personne concernée découle l'exercice d'autres droits tels que le droit de rectification, d'opposition, etc.

Il est intéressant de relever que la Cour de justice de l'Union européenne a considéré, dans un arrêt du 7 mai 2009, que :

[74] Voy. Bruxelles (9e ch.), 9 mai 2012, inédit.

« 49. Ce droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés. Ainsi qu'il est énoncé au quarante et unième considérant de la directive, afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement.

50. À cet égard, l'article 12, sous a), de la directive prévoit un droit d'accès aux données de base ainsi qu'à l'information sur les destinataires ou les catégories de destinataires auxquels ces données sont communiquées.

51. Ce droit d'accès est nécessaire pour permettre à la personne concernée d'exercer les droits visés à l'article 12, sous b) et c), de la directive, à savoir, dans le cas où le traitement de ses données ne serait pas conforme à cette directive, celui d'obtenir que le responsable du traitement rectifie, efface ou verrouille ses données [sous b)] ou qu'il notifie aux tiers auxquels les données ont été communiquées ces rectification, effacement ou verrouillage, si cela ne s'avère pas impossible ou ne présuppose pas un effort disproportionné [sous c)].

52. Ce droit d'accès est également nécessaire pour permettre à la personne concernée d'exercer le droit d'opposition au traitement de ses données à caractère personnel visé à l'article 14 de la directive ou le droit de recours en cas de dommage subi prévu aux articles 22 et 23 de celle-ci.

53. S'agissant du droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données de base ainsi que sur le contenu des données communiquées, la directive ne précise pas si ce droit concerne le passé ni, le cas échéant, la période visée dans le passé.

54. À cet égard, il convient de constater que, pour assurer l'effet utile des dispositions visées aux points 51 et 52 du présent arrêt, ce droit doit nécessairement concerner le passé. En effet, si tel n'était pas le cas, la personne intéressée ne serait pas en mesure d'exercer de manière efficace son droit de faire rectifier, effacer ou verrouiller les données présumées illicites ou incorrectes ainsi que d'introduire un recours juridictionnel et d'obtenir la réparation du préjudice subi.

[...]

70. Il y a lieu, dès lors, de répondre à la question posée de la manière suivante :

– L'article 12, sous a), de la directive impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Il appartient aux États membres de fixer un délai de conservation de cette information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement.
– Une réglementation limitant la conservation de l'information sur les destinataires ou les catégories de destinataires des données et le contenu des données transmises à une durée d'un an et limitant corrélativement l'accès à cette information, alors que les données de base sont conservées beaucoup plus longtemps, ne saurait constituer un juste équilibre des intérêt et obligation en cause, à moins qu'il ne soit démontré qu'une conservation plus longue de cette information constituerait une charge excessive pour le responsable du traitement. Il appartient à la juridiction nationale d'effectuer les vérifications nécessaires »[75].

Si, bien entendu, la Cour a fondé son raisonnement sur la directive 95/46, il est transposable en droit belge.

À noter que le droit d'accès peut être différé en cas de recherche médico-scientifique dans certaines conditions[76]. Il s'agit d'un droit différé et non pas d'une extinction du droit.

B. Détermination des finalités

38. L'article 4, 2° prescrit que les données à caractère personnel doivent être collectées pour des finalités déterminées. Cela permettra, en effet, aux personnes concernées de connaître l'objectif poursuivi par le responsable de traitement.

La détermination de la finalité est fondamentale, car c'est elle qui va déterminer le traitement de données à caractère personnel et permettre à la personne concernée de contrôler le sort réservé aux données le concernant.

La finalité doit être précise afin de permettre à la personne concernée d'effectuer cette analyse et d'exercer les droits qui lui sont conférés par la loi. Cette

[75] C.J.C.E., *Rijkeboer c. Pays-Bas*, C-553/07, http://curia.europa.eu/juris/document/document_print.jsf?doclang=FR&text=&pageIndex=0&part=1&mode=lst&docid=74028&occ=first&dir=&cid=177376.

[76] Article 10, § 2, de la loi « vie privée ».

précision permettra également au responsable de traitement de déterminer les données qui devront être collectées et traitées. Il s'agit donc d'une étape essentielle en matière de protection des données à caractère personnel.

À noter que cette finalité doit être reprise dans la déclaration de traitement afin d'également permettre à la Commission de la protection de la vie privée d'effectuer un contrôle.

39. La finalité doit également être explicite, ce qui signifie qu'elle doit être annoncée, ne pas être tenue « secrète » ou « camouflée »[77].

Il est également utile de rappeler que la finalité doit être légitime, ce qui signifie que :

> « la finalité ne peut induire une atteinte disproportionnée aux intérêts de la personne concernée par les données, au nom des intérêts poursuivis par le responsable du traitement. La notion de légitimité invite donc à un examen de proportionnalité. On n'admettra pas comme légitime un objectif qui causerait une atteinte excessive aux personnes concernées »[78].

40. La détermination de la finalité permettra également de définir une durée de conservation des données dès lors que l'article 4, 5° de la loi « vie privée » prescrit que les données à caractère personnel doivent être :

> « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. [...] »

Nous constatons que cette conservation dépendra de la finalité sous réserve de précision apportée par l'arrêté royal concernant la conservation de données « au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques »[79].

C. Nécessité/proportionnalité

41. La notion de proportionnalité se place à deux niveaux dans la loi « vie privée », à savoir celui des données à caractère personnel, mais également du traitement lui-même.

42. L'article 4, 3° prescrit que les données à caractère personnel doivent être « non excessives au regard des finalités pour lesquelles elles sont obtenues et

[77] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, 2005, p. 157.

[78] C. DE TERWANGNE, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », *Cabinet d'avocats et technologies de l'information : balises et enjeux*, 2005, p. 157 avec notes infrapaginales.

[79] Article 4, 4°, de la loi « vie privée ».

pour lesquelles elles sont traitées ultérieurement ». Cela signifie que le responsable de traitement ne pourra pas collecter des données qui ne seraient pas nécessaires pour atteindre la finalité qu'il a préalablement déterminée.

Un arrêt a été rendu par la Cour constitutionnelle dans le cadre d'une requête en annulation déposée contre la loi du 21 janvier 2010 modifiant la loi du 25 juin 1992 sur le contrat d'assurance terrestre en ce qui concerne les assurances du solde restant dû pour les personnes présentant un risque de santé accru. En vertu de cette loi, la Commission des assurances devait établir un code de bonne conduite à défaut de quoi le Roi était habilité à régler la question des questionnaires médicaux dans le cadre des assurances du solde restant dû pour les personnes présentant un risque de santé accru.

La Cour a considéré que :

> « le législateur a pu estimer que l'utilisation de ces questionnaires devait être réglementée afin d'éviter que, dans le cadre de la conclusion d'un contrat d'assurance, des questions soient posées qui ne sont pas pertinentes ou qui sont excessives et qu'il soit ainsi porté atteinte de manière disproportionnée au droit au respect de la vie privée des intéressés. Il a également pu estimer que le fait que les assureurs exigent un examen médical complémentaire et demandent les résultats de celui-ci, en plus de l'utilisation d'un questionnaire médical, pouvait constituer une restriction disproportionnée du droit au respect de la vie privée de l'intéressé dans les cas où le montant assuré demeure limité »[80].

Elle a ainsi clairement rappelé que la proportionnalité devait être analysée au niveau des données afin d'éviter que des données non nécessaires à la finalité ne soient traitées.

La Cour européenne des droits de l'homme a également précisé que :

> « Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (préambule et article 5 de la Convention sur la protection des données et principe 7 de la recommandation R.(87)15 du Comité des ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police) »[81].

[80] C.C. (166/2011), 10 novembre 2011, www.const-court.be, B.16.7.

[81] Cour eur. D.H., *S. et Marper c. Royaume-Uni* (requêtes n°s 30562/04 et 30566/04), 4 décembre 2008, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052, al. 103.

Nous constatons donc, et pour rappel, que la détermination de la finalité est primordiale pour permettre, d'une part, au responsable de traitement de déterminer les données à caractère personnel qu'il collectera et traitera ainsi que la durée de conservation de celles-ci et, d'autre part, à la personne concernée d'exercer son contrôle via les droits qui lui sont offerts par la loi « vie privée ».

43. Par ailleurs, la loi « vie privée » met également la notion de nécessité au niveau du traitement lui-même. Ainsi, les articles 5 et suivants de la loi mettent comme condition de légitimité du traitement la nécessité de celui-ci pour certaines finalités.

Dans un arrêt du 10 novembre 2011, la Cour constitutionnelle a eu l'occasion de rappeler que « toute ingérence des autorités dans le droit au respect de la vie privée [doit être] prévue par une disposition législative suffisamment précise »[82] outre qu'elle doit répondre « à un besoin social impérieux » et qu'elle doit être « *proportionnée au but légitime qui est poursuivi* »[83].

La Cour européenne des droits de l'homme a également estimé que :

> « le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique »[84].

Le juge devra donc, s'il est saisi dans le cadre d'une violation de la loi « vie privée », analyser le traitement afin de déterminer si la condition de nécessité/proportionnalité a effectivement été rencontrée.

D. Légitimité

44. La légitimité est principalement présente aux articles 5, 6, 7 de la loi « vie privée » dès lors que ces articles prévoient des situations que le législateur a considérées comme respectant la balance entre les intérêts du responsable de traitement et ceux de la personne concernée. Il s'agit, à chaque fois, d'une légitimité présumée ; légitimité qui doit être une caractéristique de la finalité visée à l'article 4 de la loi tel que cela a été mentionné ci-dessus.

[82] C.C. (166/2011), 10 novembre 2011, www.const-court.be, B35.3. Il faut relever que cette exigence permet au justiciable de pouvoir contrôler l'ingérence et sa légalité. Voy. également Cour eur. D.H., *Rotaru c. Roumanie*, du 4 mai 2000, *Rev. trim. dr. h.*, 2001, pp. 137-183, obs. O. De Schutter.

[83] Nous soulignons.

[84] Cour eur. D.H., *S. et Marper c. Royaume-Uni* (requêtes n°s 30562/04 et 30566/04), 4 décembre 2008, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052, al. 125.

La lecture de la loi doit donc être la suivante, et c'est peut-être cela qui la rendra plus aisée à lire :

1. vérifier que les données sont traitées loyalement et licitement ;
2. vérifier que les finalités sont déterminées, explicites et légitimes ;
3. pour ce dernier point, appliquer les articles 5 et suivants selon le type de données à caractère personnel pour vérifier les bases de légitimité présumée ;
4. cette étape accomplie, revenir à l'article 4 pour vérifier que les données sont bien pertinentes, adéquates, etc.

Il s'agit d'un « jeu de piste », mais qui doit être « joué » dans cet ordre pour pouvoir arriver à une solution qui soit compatible avec la loi « vie privée ».

E. Catégories de données

45. La loi « vie privée » distingue plusieurs catégories de données dont le traitement a des bases de légitimation différentes.

46. La première catégorie est celle que nous appellerons normales dès lors que les données y reprises ne sont pas susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée. Il s'agit d'une catégorie « par défaut » dès lors que s'y retrouvent toutes les données qui ne sont pas visées par les articles 6, 7 et 8 de la loi « vie privée ». Nous y retrouvons donc les noms, prénoms, adresse, etc.

Nous devons relever que le principe de traitement concernant cette première catégorie est celui d'autorisation via l'article 5, f, de la loi qui prescrit que le traitement de données à caractère personnel peut être effectué « lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi ». Cela revient à dire que le traitement est autorisé après que le responsable de traitement ait effectué une mise en balance entre ses intérêts à traiter les données et l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

En cas de litige porté devant lui par une personne concernée qui estimerait avoir été victime d'un traitement basé sur cet article, le juge devra procéder lui-même à cette analyse de balance. Il s'agira alors d'un contrôle *a posteriori*.

C'est à cette analyse *a posteriori* que la Cour d'appel de Liège a procédé, dans le cadre d'un dossier de promotion et de prospection commerciale, pour consi-

dérer que « s'il peut être admis que les finalités de promotion et de prospection commerciale sont légitimes, elles sont néanmoins primées par les droits fondamentaux de la personne concernée, dont le droit à la protection de sa vie privée »[85]. Si cette analyse *a posteriori* n'est pas confortable pour le responsable de traitement, il s'agit de la seule protection possible des intérêts et droits fondamentaux de la personne concernée.

47. Le deuxième type de catégories concerne les données que l'on qualifiera de sensibles et dont le traitement est prévu aux articles 6, 7 et 8 de la loi « vie privée ». Ces articles mettent en place un régime d'interdiction de traitement compte tenu du fait que les données visées sont susceptibles *in se* de porter atteinte aux libertés fondamentales ou à la vie privée. La loi « vie privée » prévoit des exceptions à l'interdiction qui sont principalement fondées sur une base contractuelle, une loi, un intérêt public ou un intérêt vital ou encore sur le consentement de la personne concernée. À noter que le consentement n'est pas prévu par l'article 8[86].

Il est utile d'attirer l'attention du lecteur sur le fait que, si le consentement de la personne concernée est un reflet du principe d'autodétermination de l'individu tel que nous l'avons évoqué plus haut, il constitue cependant la base de légitimation du traitement la plus faible dès lors que la personne concernée peut le retirer sans devoir motiver sa décision.

L'article 6 concerne 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 » et dont le traitement est interdit sauf à se trouver dans une des situations prévues par l'article.

L'article 7 concerne, quant à lui, les données à caractère personnel relatives à la santé dont le traitement est également, et par principe, interdit. La loi prévoit cependant des exceptions qui y sont reprises.

La troisième catégorie de données à caractère personnel sensibles concerne celles « 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 » tel que cela est visé à l'article 8 de la loi « vie privée ». Le nombre d'exceptions prévues pour traiter ces données est très faible par rapport à celles prévues aux articles 6 et 7. En effet, l'on passe de dix – douze exceptions à seulement cinq. Cela démontre l'extrême sensibilité de ces données à caractère

[85] Liège (7e ch.), 19 novembre 2009, *DAOR*, p. 455.

[86] 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.

personnel qui doivent être protégées de manière encore plus forte. À noter que la notion de nécessité est omniprésente à l'instar des deux précédentes catégories de données sensibles.

48. À ce stade-ci de la réflexion, il nous paraît utile de relever l'ambiguïté des articles 6 et 7 par rapport à leur qualification même. En effet, ces deux articles sont applicables dès l'instant où un traitement porte sur les données visées, même si le traitement ne vise pas les données à caractère personnel pour ce qu'elles sont.

Par exemple, le site internet d'une société comprend un annuaire des personnes travaillant en son sein ; cet annuaire est accompagné de leurs photos. Si un des employés apparaît sur la photo en portant des signes religieux, le traitement de cette photo, étant une donnée à caractère personnel, devrait tomber dans le champ d'application de l'article 6 dès lors que la donnée est relative à l'appartenance religieuse de la personne concernée alors qu'il importe peu au responsable de traitement que cette personne soit d'une religion ou d'une autre. Cela implique cependant que le traitement devra répondre à une des causes de légitimation prévues à l'article 6 qui pourrait être le consentement de la personne concernée, avec la faiblesse que cela comporte tel que cela a été mentionné plus haut.

Il eut été plus opportun de rédiger ces articles afin de viser le contenu des données de manière à ce que l'interdiction de traitement soit le principe pour les données à caractère personnel relatives à la santé si elles sont traitées pour ce qu'elles révèlent ou contiennent. Cela enlèverait l'ambiguïté relevée ci-dessus et que nous retrouvons également dans la directive 95/46.

Le juge devra donc, à nouveau, analyser la question de manière contextuelle afin d'échapper à cette ambiguïté que nous venons d'examiner.

49. À noter également que l'arrêté royal précise certains éléments de ces articles consacrés aux données à caractère personnel sensibles.

F. Sécurité et confidentialité

50. La confidentialité peut être définie soit comme « la sécurité visant à interdire l'accès à un système informatique »[87] soit comme « le caractère d'une information confidentielle »[88].

En réalité, l'article 16 de la loi « vie privée » vise tant la confidentialité que la sécurité du traitement à deux niveaux, à savoir aux niveaux organisationnel et technique.

[87] *Larousse*, www.larousse.fr/dictionnaires/francais/confidentialit%C3 %A9.

[88] *Larousse*, www.larousse.fr/dictionnaires/francais/confidentialit%C3 %A9.

À noter que la Cour européenne des droits de l'homme considère que la confidentialité et la sécurité sont des éléments essentiels.

Elle a ainsi considéré que :

> « La législation interne doit ménager des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention (arrêt Z c. Finlande du 25 février 1997, Recueil des arrêts et décisions 1997-I, p. 347, § 95) »[89].

51. D'un point de vue organisationnel, le responsable de traitement doit s'assurer que les personnes agissant sous son autorité soient informées des dispositions de la loi « vie privée », de son arrêté royal et de toutes dispositions pertinentes[90].

Il doit également veiller à mettre en place une structure ou une organisation pour éviter la perte de données, des destructions ou des modifications de données non autorisées, des accès non autorisés, etc.

En d'autres termes, il devra prendre des dispositions en termes d'organisation qui garantira la personne concernée contre de tels faits. Par exemple, le responsable de traitement devra s'assurer que seules les personnes devant effectivement avoir accès à des données à caractère personnel y aient effectivement accès à l'exclusion des autres. Il lui appartiendra donc de prévoir une organisation adéquate et efficace.

Cette notion de sécurité/confidentialité organisationnelle peut également être expliquée à travers l'exemple de l'utilisation des mots de passe pour accéder à un réseau protégé. Il a été constaté que certaines entreprises imposent à leurs employés de changer de mot de passe tous les mois sans pouvoir choisir un mot de passe qu'ils auraient déjà utilisé durant les six derniers mois. Si le principe peut paraître intéressant pour éviter l'usurpation d'identité sur le réseau informatique de la société, cela s'avère, en réalité, une catastrophe. En effet, l'on constate que les employés écrivent leur mot de passe sur un papier collé à leur ordinateur pour être certains de ne pas l'oublier, compte tenu du rythme de changement de mot de passe imposé. Cette organisation au niveau des mots de passe est donc totalement contre-productive dès lors que le système d'information n'est plus protégé de manière efficace, et le responsable de traitement contreviendrait donc à son obligation de sécurité/confidentialité sans s'en rendre compte.

[89] Cour eur. D.H., *M. S. c. Suède* (74/1996/693/885), 27 août 1997, http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-62738, § 41.

[90] Article 16, § 2, 3°, de la loi « vie privée ».

Ce niveau organisationnel se retrouve également au stade de la formation des personnes à n'accéder qu'aux données à caractère personnel dont elles ont réellement besoin. Par exemple, en matière de données relatives à la santé, le responsable de traitement devra s'assurer que son personnel médical n'accédera que, d'une part, aux données des patients dont ils assurent le suivi thérapeutique et, d'autre part, aux seules données de ces patients dont ils ont besoin dans le cadre du suivi thérapeutique.

Le responsable de traitement devra également « 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 »[91]. Il s'agit également de mesures organisationnelles.

52. Au niveau technique, le responsable de traitement devra s'assurer qu'il a mis en place des mesures adéquates de protection de ses traitements d'un point de vue technique.

Ainsi, il devra s'assurer que son système informatique réunit les mesures nécessaires à éviter toute intrusion non autorisée via une bonne gestion d'accès, toute perte, destruction ou modification de données, etc.

À noter que la notion de sécurité s'entend aussi des accès physiques au réseau informatique du responsable de traitement. Il faudra donc être attentif à ce que l'accès au serveur, par exemple, soit réglementé et qu'il ne soit ouvert qu'aux seules personnes qui ont la nécessité d'y accéder. Il serait bien inutile de prévoir des règles d'accès strictes aux données si le serveur les contenant n'était pas suffisamment protégé et pouvait être subtilisé…

Ces mesures techniques « doivent assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels »[92]. Le juge qui serait donc amené à analyser cette problématique devra tenir compte de ces différents paramètres en se plaçant au jour de la brèche dans la sécurité.

À noter qu'il s'agit d'une obligation de moyen dans le chef du responsable de traitement, mais dont il est difficile de se départir.

En effet, la loi « vie privée », prescrit que :

> « Le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi.

[91] Article 16, § 2, 1°, de la loi « vie privée ».

[92] Article 16, § 4, al. 2, de la loi « vie privée ».

Il est exonéré de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable »[93].

53. Afin de suivre la logique de la loi « vie privée », nous reparlerons brièvement de la sous-traitance et, plus particulièrement, de sa relation avec le responsable de traitement.

Pour rappel, le responsable de traitement peut faire appel à un sous-traitant en raison de ses compétences particulières dans la mise en œuvre du traitement, entre autres. La loi « vie privée » lui impose cependant de faire choix d'un sous-traitant qui « apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements »[94]. Cette responsabilité dans le choix du sous-traitant se trouve donc dans le chef du responsable de traitement qui doit en répondre à la personne concernée.

Par ailleurs, la relation entre ces deux acteurs doit faire l'objet d'un contrat prévoyant, au moins, la responsabilité du sous-traitant et de convenir avec lui qu'il « n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du paragraphe 3 [de l'article 16] »[95].

Le tout doit être « consigné par écrit ou sur un support électronique »[96].

G. Sanctions

54. Le législateur a prévu des sanctions pénales en cas d'infraction à la loi « vie privée ». Ces sanctions y sont reprises au chapitre VIII et vont de l'amende à la « confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction, tels que les fichiers manuels, disques et bandes magnétiques, à l'exclusion des ordinateurs ou de tout autre matériel, ou ordonner l'effacement de ces données » en passant par la publication du jugement soit dans son intégralité soit en extraits dans un ou plusieurs journaux.

Cette dernière peine paraît, en réalité, la plus efficace dans le chef d'entreprises qui n'auraient aucune peine à payer l'amende dont le coût aurait éventuellement été intégré dans leurs analyses de coûts/bénéfices. En effet, une entreprise pourrait faire une balance entre le bénéfice que rapporterait un traitement même illégal par rapport au coût que générerait le respect de la loi. On doit entendre le terme coût au sens large du terme et non uniquement financier. Nous nous rendons alors compte que l'amende leur importe peu. Par contre, la publication du jugement pourrait impacter les responsables de traitements

[93] Article 15*bis*, al. 2 et 3, de la loi « vie privée ».
[94] Article 16, § 1er, 1°, de la loi « vie privée ».
[95] Article 16, § 1er, 4°, de la loi « vie privée ».
[96] Article 16, § 1er, 5°, de la loi « vie privée ».

indélicats de manière beaucoup plus significative. Le juge ne devrait donc pas hésiter à utiliser cette sanction.

Une autre critique que nous pouvons formuler à l'égard du régime belge est la réticence des personnes concernées de porter plainte au regard du coût en temps et en argent qu'une telle procédure engendrerait.

55. Ce problème est également rencontré au niveau des actions civiles qu'une personne concernée pourrait porter devant les juridictions civiles et, plus particulièrement, devant le président du tribunal de première instance de son domicile siégeant comme en référé[97] pour « toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne concernée s'est opposée ou encore qui a été conservée au-delà de la période autorisée »[98] ou devant le tribunal compétent pour toute autre demande.

L'on doit cependant bien constater que le coût d'une procédure est un frein indéniable dans le chef de la personne concernée à porter le débat devant le juge. Il serait donc utile que le droit belge se dote d'un système de *class action* afin de pallier ce problème.

Une autre solution serait de voir la Commission de la protection de la vie privée faire usage des pouvoirs qui sont donnés au président de ladite Commission par l'article 32, § 3. En effet, cette disposition permet au président de soumettre au tribunal de première instance tout litige concernant l'application de la présente loi et de ses mesures d'exécution. La Commission remplirait ainsi son rôle de garant du respect de la protection des données à caractère personnel au profit des personnes concernées. Il est, bien entendu, regrettable qu'il ne soit pas fait plus souvent appel à cette compétence.

À noter qu'au pénal, la loi impose à la Commission de dénoncer au procureur du Roi les infractions dont elle a connaissance, ce qu'elle ne fait malheureusement pas non plus, contrevenant ainsi à la loi « vie privée ».

Pourtant la Commission permettrait ainsi une meilleure protection des personnes concernées. La peur du gendarme a des limites et il faut, à un certain moment, passer aux sanctions.

[97] Article 14 de la loi « vie privée ».
[98] Article 14 de la loi « vie privée ». Les pouvoirs du président devant être analysés de manière stricte, il nous paraît difficile d'utiliser cette voie pour demander réparation d'un dommage découlant d'une infraction à la loi « vie privée » à moins de considérer cette demande comme un accessoire de la demande principale qui entrerait dans la compétence du président telle que définie par la loi. Voy. à ce sujet J. Herveg, « La procédure "comme en référé" appliquée aux traitements de données », *Les actions en cessation*, Bruxelles, Larcier, 2006, pp. 215-246.

56. À ce stade-ci de notre discussion, il paraît utile de consacrer quelques lignes à la question de l'utilisation d'une preuve recueillie en violation de la loi « vie privée ».

Nous ne reviendrons pas sur la jurisprudence dite Antigone qui a déjà fait l'objet de nombreux écrits[99], mais souhaitons cependant attirer l'attention sur certaines décisions.

En matière de vidéosurveillance, la Cour de cassation a ainsi considéré que « de la seule circonstance qu'une caméra de surveillance, installée visiblement sur la voie publique, permet de réunir des éléments de preuve des infractions qui s'y commettent, il ne saurait se déduire une ingérence dans l'exercice du droit au respect à la vie privée »[100].

Un arrêt de la Cour constitutionnelle du 22 décembre 2010 a été rendu sur questions préjudicielles relatives à l'article 34, §1er, alinéa 2, de la loi du 5 août 1992 sur la fonction de police posées par le Tribunal correctionnel de Gand. Le Tribunal se posait la question d'une éventuelle violation du droit au respect de la vie privée tel que consacré par l'article 22 de la Constitution par l'article 34, § 1er, alinéa 2, de la loi du 5 août 1992 sur la fonction de police « dans l'interprétation selon laquelle la méconnaissance de celui-ci, lors d'un contrôle d'identité illégal, ne conduit pas nécessairement à la nullité de la preuve obtenue ». Par ailleurs, le Tribunal correctionnel se posait la question d'une éventuelle inégalité non autorisée entre cet article 34, § 1er, alinéa 2, dans l'interprétation mentionnée ci-dessus, dès lors que la loi ne prévoyait aucune sanction de nullité, tel que c'était le cas dans d'autres textes législatifs, alors qu'il s'agit toujours de la garantie de droits fondamentaux, ce qu'est le droit au respect de la vie privée. Après avoir énuméré plusieurs arrêts de la Cour européenne des droits de l'homme de Strasbourg relatifs à la question des éléments de preuve obtenus en méconnaissance de l'article 8 de la CEDH, la Cour considère qu'ils faisaient apparaître « d'une part, que la Cour européenne des droits de l'homme a jugé que les articles 6 et 8 de la Convention européenne ne comportent pas de règles concernant l'admissibilité d'une preuve dans une affaire et, d'autre part, que l'utilisation d'une preuve obtenue en méconnaissance de l'article 8 de cette Convention ne conduit pas nécessairement à une violation du droit à un procès équitable garanti par l'article 6.1.de la Convention européenne » .

Elle poursuit en considérant qu' « il s'ensuit que la circonstance qu'une preuve obtenue en méconnaissance d'une disposition légale visant à garantir le droit au respect de la vie privée n'est pas automatiquement nulle, ne viole pas en soi le droit au respect de la vie privée garanti par l'article 8 de la Convention

[99] Voy. entre autres B. Devos et C. Bleret, « La jurisprudence Antigone en matière de roulage », *Circulation routière et responsabilité*, coll. Recyclage en droit, Limal, Anthemis, 2012, pp. 9-46.

[100] Cass., 17 mars 2010, R.W., 2011-12 n° 30, 24 mars 2012, pp. 1332 et s.

européenne des droits de l'homme » et que « l'article 22 de la Constitution, qui garantit également le droit au respect de la vie privée, ne comporte pas plus que l'article 8 de la Convention européenne des droits de l'homme une règle explicite relative à l'admissibilité de la preuve obtenue en méconnaissance du droit garanti pour celui-ci ».

La question préjudicielle a donc reçu une réponse négative dès lors que l'article 22 de la Constitution « n'exige pas en soi qu'une preuve obtenue en méconnaissance du droit qu'il garantit doit être considérée comme nulle en toute circonstance ».

L'on constate donc que la fin justifie les moyens ayant pour conséquence que la protection de la vie privée et des données à caractère personnel s'efface bien souvent face à ce principe[101].

Conclusions

57. Eu égard au fait que tant la définition de données à caractère personnel que celle de traitement soient extrêmement larges, la loi « vie privée » trouve à s'appliquer dans de nombreuses matières. Il s'agit réellement d'une loi transversale venant s'appliquer parallèlement à d'autres dispositions.

Elle offre également des possibilités aux plaideurs par rapport à l'exercice de certains droits et à l'accès à certaines données concernant leurs clients.

Par ailleurs, ce droit est en mutation constante par le travail de la jurisprudence tant nationale qu'internationale.

58. Nous rappelons également que la loi « vie privée » doit faire l'objet d'une analyse contextuelle, ainsi que nous l'avons relevé ci-dessus, afin d'éviter qu'elle ne soit contre-productive.

À cela s'ajoute la nécessité de voir la Commission de la vie privée user – mais pas abuser – de ses pouvoirs afin de porter devant les autorités judiciaires les cas de violation de la loi « vie privée » afin que les contrevenants n'aient pas un sentiment d'impunité qui porte préjudice à la protection des données à caractère personnel, protection qui est pourtant un droit fondamental.

59. Nous ne pouvons pas terminer cette contribution sans évoquer une éventuelle mutation majeure de la loi « vie privée ». En effet, l'Union européenne travaille sur une réforme majeure de la directive 95/46, réforme qui devrait avoir, si elle se réalise, un impact important sur le droit belge. En effet, la loi

[101] Voy. également, à ce sujet, C. de Terwangne, J. Herveg, J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication : introduction à la protection des données dans la preuve des causes de divorce*, Kluwer, 2005.

serait remplacée par un règlement européen[102] censé harmoniser totalement le droit européen en la matière.

L'instrument utilisé montre que l'Union européenne, et singulièrement sa Commission, veut avoir la mainmise sur la matière via tant le règlement que les actes délégués qui y sont prévus. Ces derniers posent cependant problème au niveau de la prévisibilité à laquelle tout citoyen est en droit de s'attendre et qui est requise par l'article 8 de la CEDH.

À l'heure actuelle, nous ne pouvons pas en dire beaucoup plus dès lors que ce projet suit son parcours parlementaire au sein du Parlement européen. L'on peut cependant dire que la Commission européenne a la volonté de faire adopter ce texte, qui est bien imparfait à plusieurs égards mais qui tend vers une protection harmonisée des données à caractère personnel en Europe, pour 2014, c'est-à-dire demain.

[102] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.