Le 'cloud computing' ou l'informatique dématérialisée: la protection des données au cœur de la relation contractuelle[1]

Benjamin Docquir[2]

RÉSUMÉ

Le phénomène du cloud computing connaît une importance croissante et s'impose peu à peu comme une alternative crédible pour les entreprises, en dépit des craintes suscitées par le fait que les données sont hébergées chez un fournisseur tiers. Dans un tel contexte, il semble utile de clarifier les règles pertinentes en matière de protection des données à caractère personnel, au cœur des interrogations suscitées par la perte de maîtrise sur les données. Il n'y va pas seulement des droits et libertés des individus concernés, mais aussi de la préservation de l'équilibre contractuel entre le fournisseur et l'utilisateur de ces services d'informatique dématérialisée.

SAMENVATTING

Cloud computing is een snel groeiend verschijnsel dat stilaan een plaats verwerft als geloofwaardig alternatief voor bedrijven, ondanks de bezorgdheid die wordt opgewekt omdat gegevens bij een externe leverancier worden bewaard. In deze context lijkt het nuttig om de relevante regels betreffende de bescherming van persoonsgegevens te verduidelijken. Zij staan immers centraal in het debat over het verlies aan controle over de gegevens. Het gaat niet alleen om de rechten en vrijheden van de betrokkenen, maar ook over het behoud van het contractuele evenwicht tussen de leverancier en de gebruiker van deze nieuwe informaticadiensten.

1. Une version en néerlandais du présent texte est publiée dans le *Cahier du Juriste – van de jurist*, 2011/4, p. 105.
2. Avocat au barreau de Bruxelles, Simont Braun, et collaborateur scientifique à l'Université Libre de Bruxelles, Unité de droit économique.

I. INTRODUCTION

1. Le cloud computing constitue sans nul doute une étape importante dans l'histoire de l'informatique, et sa mise en œuvre peut entraîner des changements majeurs dans la gestion et l'organisation de l'informatique d'entreprise.

Sur le plan juridique, l'une des principales interrogations suscitées par le phénomène concerne la protection des données, qui sont hébergées chez le fournisseur et non plus sur les serveurs de l'entreprise utilisatrice. Dans la mesure où les informations ainsi externalisées constituent des données à caractère personnel, ce qui sera, en règle, le cas, se pose avec acuité la question du régime de protection découlant de l'application de la loi dite 'vie privée' du 8 décembre 1992[3].

Dans la présente étude, nous aborderons cette question essentiellement en vue de délimiter les droits et devoirs respectifs de l'utilisateur du cloud computing et du fournisseur de tels services. Nous examinerons aussi l'impact potentiel de ce régime impératif sur la relation contractuelle entre l'utilisateur et le fournisseur de cloud computing.

II. BRÈVE PRÉSENTATION DU CLOUD COMPUTING

2. Pour commencer, présentons brièvement les caractéristiques principales du phénomène du cloud computing, ainsi que les particularités du modèle économique qui en découle[4].

A. Un 'nuage', pour quoi faire?

3. L'on parle de 'nuage' (*cloud*, en anglais) car c'est généralement par un pictogramme en forme de nuage que les informaticiens représentent le réseau Internet. Or, le *cloud computing* permet à l'utilisateur, ni plus ni moins, de placer l'ensemble de ses ressources informatiques au sens large (serveurs, outils de développement, applications, données, etc.) dans un *data center* géré par le fournisseur, pour y accéder par le biais d'une simple connexion Internet et d'un logiciel de navigation. En d'autres termes, l'entreprise qui recourt au cloud computing peut renoncer à tout ou partie de son infrastructure de serveurs propres. Elle n'en aura plus besoin, puisque le fournisseur se charge de mettre à sa disposition espaces de stockage, capacités de traitement, données et logiciels d'application, le tout sur des serveurs situés dans des *data centers* dont ce fournisseur ou un tiers assurent eux-mêmes le bon fonctionnement et l'entretien. De même, le particulier qui utilise des services de cloud computing ne doit plus se soucier de la sauvegarde de ses données, photos, messages ou autres documents, puisque le tout est stocké par le fournisseur, 'dans les nuages', ou plus précisément sur une petite partie d'une infrastructure de serveurs mise à sa disposition[5].

4. Ainsi, l'entreprise peut bénéficier d'un accès à ses données et à ses applications à tout moment, quel que soit le lieu où se trouvent ses collaborateurs, sans devoir entretenir des infrastructures dont elle n'a pas nécessairement un besoin permanent. Elle peut augmenter ou diminuer le volume qu'elle 'consomme' en fonction de ses besoins réels du moment, et, de façon plus générale, convertir certaines dépenses d'investissement de capital en dépenses d'exploitation.

5. On distingue généralement trois modèles différents, selon la nature des services offerts par le fournisseur: dans le modèle dit *Infrastructure as a Service* ('IaaS'), le fournisseur donne 'uniquement' accès à des serveurs virtuels, sur lesquels l'utilisateur peut installer ses propres logiciels et systèmes d'exploitation; dans le modèle *Platform as a Service* ('PaaS'), le fournisseur donne accès à un environnement de développement, ce qui permet à l'utilisateur de développer beaucoup plus rapidement ses propres applications, mais en respectant les contraintes propres à la plate-forme en question; enfin, dans le modèle *Software as a Service* ('SaaS'), sans doute le plus connu du grand public, le fournisseur donne accès à une ou des applications, directement exploitables. Typiquement, des outils de travail collaboratif et de communication entre les collaborateurs peuvent être

3. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (*MB* 18 mars 1993, p. 5.801), modifiée principalement par la loi du 11 décembre 1998 (*MB* 3 février 1999, p. 3.049), transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.

4. Nous renvoyons le lecteur intéressé par les aspects techniques ou organisationnels du cloud computing au livre de G. PLOUIN, *Cloud Computing. Une rupture décisive pour l'informatique d'entreprise*, 2ème éd., Dunod, 2011. On consultera également avec intérêt, entre autres études, celles de l'agence européenne ENISA (European Network and Information Security Agency), notamment *Security & Resilience in Governmental Clouds*, Janvier 2011, disponible sur http://enisa.europa.eu.

5. Dans la présente étude, nous nous concentrerons sur les cas d'utilisation du cloud computing par les entreprises et les organisations, à des fins professionnelles. Le recours au cloud computing par les particuliers, à des fins privées, pose des questions spécifiques sur lesquelles nous ne pouvons nous étendre ici. Pour n'en dire qu'un seul mot, nombre de services de cloud computing sont accessibles gratuitement pour un usage privé, le fournisseur se rémunérant par d'autres voies telles que la publicité ou divers services annexes. A ce sujet, voy. A. STROWEL et J.-P. TRIAILLE (dir.), *Google et les nouveaux services en ligne*, Bruxelles, Larcier, 2008.

placés dans le cloud. Mais d'autres exemples, tels que le recours à des applications de type 'CRM' (*customer relationship management*), de mailings de masse, ou encore des solutions de paiement en ligne ou de stockage de documents, sont déjà aujourd'hui une réalité.

Précisons aussi que certains fournisseurs, à côté du logiciel qu'ils éditent et mettent à disposition sur une plate-forme SaaS, permettent à des éditeurs tiers de développer des applications (éventuellement accessoires ou complémentaires à un logiciel principal) qui seront également accessibles et utilisables en mode SaaS sur la même plate-forme (du type *salesforce.com* ou *Google Apps*).

6. Comme on le voit, une caractéristique marquante du cloud computing est la multiplicité et, subséquemment, l'opacité relative des acteurs auxquelles l'utilisateur peut se trouver confronté: ainsi, un service de stockage de documents ou de photos qui développe sa propre application et la commercialise en mode *software as a service* peut utiliser l'infrastructure d'un autre fournisseur (*infrastructure as a service* ou *platform as a service*); de même, une plate-forme de services peut donner accès à des logiciels édités par différents éditeurs, et l'utilisateur peut encore choisir d'installer sur la plate-forme qu'il loue un logiciel spécifique développé par un tiers ou par lui-même. Dans ces conditions, le paradigme du cloud computing ne correspond évidemment pas à une qualification juridique unique et homogène. Il est indispensable d'analyser avec soin les particularités et les circonstances de fait propres à chaque cas d'espèce.

B. Avantages et inconvénients

7. On l'aura compris, la caractéristique essentielle de l'informatique dématérialisée est que le fournisseur prend en charge la gestion et l'entretien (la 'maintenance') des serveurs, et se spécialise sur la mise à disposition d'une infrastructure technique et de moyens d'accès à cette infrastructure. En pratique, le *cloud computing* est ainsi une forme particulière d'externalisation des infrastructures et des services informatiques d'un particulier, d'une organisation ou d'une entreprise. L'utilisateur a ainsi accès à des ressources qu'il ne pourrait pas nécessairement s'offrir et, surtout, il peut réaliser des économies non négligeables. Celles-ci tiennent déjà à la simplification du système d'information, puisqu'il suffit en principe de conserver des postes de travail et une connexion Internet. Des gains de temps et d'efficacité peuvent aussi émerger de la plus grande facilité dans le développement et le déploiement de nouvelles applications. En bref, l'utilisateur peut ainsi se concentrer sur son cœur de métier, et laisser à des prestataires spécialisés le soin de sélectionner, d'entretenir et de développer les infrastructures, les outils de développement et les applications nécessaires au bon fonctionnement de son système d'information.

8. Un autre avantage commercial mis en avant par les partisans du cloud computing est la flexibilité et la souplesse avec lesquelles l'utilisateur peut avoir accès à des ressources ou des services, de manière rapide et immédiate, à la demande, indépendamment du lieu où il se trouve. En particulier, l'utilisateur peut ainsi très aisément dimensionner les ressources dont il a besoin, et notamment les faire évoluer en cas de montée en charge rapide (p. ex., l'exploitant d'un site de commerce électronique qui doit pouvoir supporter des visites beaucoup plus importantes lors de pics de ventes annuelles). De plus, les ressources mises 'dans le nuage' peuvent être consultées et exploitées par différents utilisateurs en même temps, y compris par les travailleurs dits 'nomades' de l'entreprise.

9. L'utilisateur peut opter pour un cloud public (ou 'externe'), mis à disposition de différents clients par le fournisseur, et dans lequel les logiciels et les données sont entièrement hébergés sur l'infrastructure (externe) du fournisseur, ou pour un cloud privé, à savoir une plate-forme technique, gérée en interne par l'entreprise, voire par une division ou une autre société du groupe, mais en tout cas destinée à ne recevoir que les données et les applications d'un seul utilisateur. Entre ces deux extrêmes, il est aussi possible de recourir à un cloud dit 'communautaire', à savoir une infrastructure ou une plate-forme gérée par plusieurs organisations ayant des intérêts communs, ou encore au cloud dit 'hybride', qui ne serait autre qu'une combinaison des clouds 'privé' et 'public' (p. ex. dans le but de stocker certaines données sensibles sur un cloud privé). A vrai dire, les combinaisons possibles sont nombreuses et dépendent des configurations techniques et commerciales disponibles sur le marché ainsi que des contraintes propres à chaque utilisateur.

10. Reflet de cette 'élasticité', le modèle économique de beaucoup de prestataires de cloud computing repose sur une formule de paiement à l'utilisation. Ceci permet, en principe, de réduire les coûts totaux pour l'utilisateur, à condition bien entendu de convenir de modes de calcul adaptés, qui permettent réellement d'ajuster les prix aux besoins réels de l'entreprise.

C. Interrogations suscitées par le cloud computing

11. L'une des métaphores les plus éloquentes pour décrire le phénomène du cloud computing est celle de l'électricité: l'entreprise ou l'organisation choisit d'externaliser la production des ressources informatiques 'de base' vers des producteurs dont c'est le métier principal. Dans cette analogie, l'accès à des capacités de calcul et à des ressources de stockage devrait être aussi simple que l'accès à des ressources comme l'eau ou l'électricité. La réalité, à n'en pas douter, est autrement complexe, mais l'image a le mérite de frap-

per les esprits et d'attirer l'attention sur certains enjeux fondamentaux du cloud computing.

12. Pour une large partie, le cloud computing repose sur des techniques connues depuis plusieurs années. Il ne représente pas tant une avancée scientifique nouvelle, que l'émergence d'un nouveau modèle d'accès aux ressources informatiques et de nouveaux modèles économiques, exploitant les capacités nouvelles des réseaux de communications électroniques[6].

13. Sur un plan juridique, en revanche, le phénomène du cloud computing pose un certain nombre de questions importantes et nouvelles. L'on songe, bien sûr, à l'équilibre contractuel entre l'utilisateur et le fournisseur, fortement influencé par la perte de maîtrise de l'utilisateur sur ses données; l'on songe également aux questions de protection des données et de sécurité, en particulier pour des catégories de données soumises à une réglementation particulière, comme par exemple les données en matière financière et fiscale ou celles relevant du domaine de la santé[7]; mais de façon plus générale, dès lors qu'un nombre croissant de données sont stockées sur des serveurs accessibles à distance, se pose la question de l'accès à ces données par des tiers, notamment les services de police et de renseignement[8], y compris ceux d'Etats étrangers[9]. Ne fût-ce que pour cette dernière raison, les pouvoirs publics ont manifestement un rôle à jouer dans l'encadrement réglementaire du cloud computing. C'est ainsi que l'on a appris récemment que la France envisage de créer son propre 'cloud', en mettant sur pied un réseau de *data centers* destiné à accueillir les données des pouvoirs publics ou d'entreprises, jugées trop stratégiques que pour être stockées sur les systèmes d'entreprises américaines ou d'autres pays[10], tandis que le gouvernement néerlandais envisagerait d'interdire aux administrations le recours aux services de cloud computing de certains opérateurs établis à l'étranger et susceptibles de faire l'objet de saisies ou de mesures de communication des données dans le cadre du Patriot Act américain[11].

14. La présente étude aborde essentiellement la question de la protection des données à caractère personnel placées 'dans le nuage', au regard de la loi du 8 décembre 1992[12], qui transpose la directive 95/46[13], et sous l'angle des relations contractuelles entre l'utilisateur et le fournisseur de cloud computing.

III. PROTECTION DES DONNÉES: LES ASPECTS RÉGLEMENTAIRES

15. Les données hébergées chez un fournisseur de cloud computing passent entre les mains d'un grand nombre d'opérateurs: l'entreprise ou l'organisation qui les utilise, le fournisseur de cloud computing, les intermédiaires fournissant l'accès au réseau de communications électroniques, les sous-traitants éventuels du fournisseur de cloud computing, etc. Face à cette multiplicité d'acteurs, il convient d'identifier les rôles et les responsabilités de chacun en termes de respect des règles de protection des données. Ceci constitue l'une des principales difficultés dans l'application de la loi du 8 décembre 1992 au contexte du cloud computing. Il s'agit toutefois d'un préalable indispensable si l'on veut assurer le respect du régime de protection des données imposé par la loi précitée.

---

6. L. FERREIRA PIRES, "Wat is cloud computing?", *Computerrecht*, 2011/63, p. 104.
7. A propos des données relatives au patient détenues par un hôpital, voy. J.-M. VAN GYSEGHEM, "Cloud computing et protection des données à caractère personnel: mise en ménage possible?", *RDTI* 2011, n° 42, pp. 35 et s., spéc. n^{os} 15 et 16.
8. A cet égard, on notera l'importance de la décision de la Cour de cassation du 18 janvier 2011, RG P.10.1347.N, en cause de *Yahoo! Inc. / Min. P.* Dans cette affaire, la Cour de cassation analyse la portée de l'art. 46*bis* du Code d'instruction criminelle, et conclut que le devoir de collaboration avec le parquet imposé par cette disposition ne s'applique pas uniquement aux fournisseurs de réseaux et services de communications électroniques au sens de la loi du 13 juin 2005 sur les communications électroniques (voy. à ce sujet la note de L. KERZMANN, sous l'arrêt, dans *RDTI* 2011, vol. 3, p. 116). Au contraire, la haute juridiction décide que cette obligation s'impose également à toute personne qui offre un service consistant en tout ou en partie dans la transmission de signaux par des réseaux de communications électroniques, et que celui qui offre un service permettant à ses clients de recevoir ou de diffuser de l'information via un réseau électronique, est également un fournisseur de services de communications électroniques.
9. Voy. les actes de la journée d'études organisée le 24 février 2011 par le Centre de Recherches Informatique et Droit et le *Queen Mary College* de Londres, intitulée "Law Enforcement in the Clouds: Regulatory Challenges"; voy. aussi I. WALDEN, *Law Enforcement Access in a Cloud Environment*, *Legal Studies Research Paper*, 74/2011, Queen Mary School of Law, disponible sur http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067.
10. LEMONDE.FR, "L'informatique dématérialisée 'à la française' aiguise les appétits", *Le Monde* 21 septembre 2011; G. DE CALIGNON, "L'Etat investira 135 millions d'euros dans l'alliance française pour le 'cloud computing'", *Les Echos*, 20 septembre 2011.
11. Selon l'article du *Monde*, précité. Des informations plus nuancées ont été données dans le cadre des questions et réponses parlementaires. Elles sont publiées sur le site Internet www.itenrecht.nl (billet n° IT 500), avec les liens pertinents.
12. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (*MB* 18 mars 1993, p. 5.801), modifiée principalement par la loi du 11 décembre 1998 (*MB* 3 février 1999, p. 3.049), transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.
13. 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 (*JOCE* 23 novembre 1995, L. 281, pp. 31-50).

A. Champ d'application de la loi du 8 décembre 1992

16. Mais avant d'analyser les rôles et responsabilités des différents acteurs, il convient de rencontrer trois objections que l'on pourrait élever à l'encontre de l'application de la loi du 8 décembre 1992 dans le contexte du cloud computing.

1. Notion de donnée à caractère personnel et possibilité concrète d'identifier les personnes concernées

17. L'on sait que la loi du 8 décembre 1992 ne s'applique qu'en présence d'un traitement automatisé de données à caractère personnel. Le stockage de données sur des serveurs distants constitue à n'en pas douter un traitement automatisé, mais de telles données constituent-elles vraiment des données à caractère personnel?

18. En vertu de la directive 95/46, l'on entend par '*donnée à caractère personnel*' toute information concernant une personne physique '*identifiée ou identifiable*', étant entendu que la 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 au sens large, est '*réputée identifiable*'. Le considérant 26 de la directive 95/46 ajoute que pour déterminer si une personne est identifiable, il y a lieu 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"*[14]. Il s'ensuit que les règles de protection des données ne sont pas applicables aux informations rendues anonymes *"d'une manière telle que la personne concernée n'est plus identifiable"*[15]. Dans la ligne de ce qui précède, le groupe de l'article 29[16], dans son avis 4/2007 sur le concept de donnée à caractère personnel[17], reconnaît que, dans certains cas, la pseudonymisation, l'anonymisation ou le cryptage des données sont susceptibles de faire perdre à une information sa qualité de donnée à caractère personnel, pour autant qu'il ne soit effectivement plus possible d'identifier la personne concernée, compte tenu de l'ensemble des circonstances de l'espèce et notamment des finalités pour lesquelles les données ainsi codées sont susceptibles d'être réutilisées ou non (en particulier, de la question de savoir si l'identification des intéressés fait partie des finalités poursuivies par la personne qui traite ou réutilise les données).

En droit belge, le rapport au Roi précédant l'arrêté royal du 13 février 2001[18] précise que l'anonymisation des données consiste à *"supprimer les données d'identification afin que les données individuelles ne puissent plus être attribuées nommément aux personnes concernées"* (en vertu du même arrêté royal, les données qui ne peuvent être mises en relation avec une personne déterminée qu'au moyen d'un code de cryptage, sont des données dites '*codées*', soumises à un régime particulier).

19. La question est donc de savoir si les données à caractère personnel chargées sur une plate-forme de cloud computing, rendues anonymes ou cryptées selon l'une ou l'autre méthode, sont toujours susceptibles de permettre l'identification des personnes concernées, que ce soit par le fournisseur, par l'utilisateur ou par un tiers, et ce compte tenu de l'ensemble des moyens qui peuvent raisonnablement être mis en œuvre. L'on peut aussi se demander si des données rendues pseudonymes ou anonymes dans certaines conditions ne devraient pas bénéficier d'un régime juridique plus souple, en particulier lorsque la personne qui traite ces données n'a pas d'accès aux moyens nécessaires pour identifier les personnes physiques. Force est en effet de constater que l'avis 4/2007 précité du groupe de l'article 29 ouvre la porte à une appréciation relative du concept de données à caractère personnel, en fonction de la personne qui traite ces données, des buts qu'elle poursuit et des moyens dont elle dispose (ou pas) pour identifier les personnes. Cette personne peut en effet être dans l'incapacité de retrouver l'identité des personnes concernées, de sorte que l'anonymisation ou le cryptage seraient bien, dans son chef, irréversibles, pour des raisons techniques (parce qu'elle ne dispose pas de la 'clé' de codage ou d'encryption) ou juridiques (parce qu'elle a pris un engagement contractuel de ne pas identifier les personnes concernées).

20. Des auteurs anglais ont étudié avec attention les aspects techniques du cryptage, de l'anonymisation et de la sauvegarde des données dans le contexte du cloud computing, notamment à la lumière de l'avis 4/2007 précité[19]. Sur cette base, ils soutiennent que dans certains cas, les données

14. Nous soulignons.
15. Considérant 26 de la directive 95/46.
16. Le groupe dit 'de l'article 29' est un organe consultatif et indépendant, composé notamment de représentants des autorités de contrôle en matière de protection des données dans les Etats membres, réglé conformément aux art. 29 et 30 de la directive 95/46. Voy. à ce propos Y. POULLET et S. GUTWIRTH, "The contribution of the article 29 working party to the construction of a harmonised european data protection system: an illustration of 'reflexive governance'" in M. VERONICA PEREZ ASINARI et P. PALAZZI (dir.), *Défis du droit à la protection de la vie privé. Perspectives du droit européen et nord-américain*, Cahiers du CRID, n° 31, Bruxelles, Bruylant, pp. 570-609.
17. Groupe de travail 'Article 29' sur la protection des données, avis 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, WP136, disponible sur http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.
18. AR 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (*MB* 13 mars 2001, p. 7.839).
19. W.K. HUON, C. MILLARD et I. WALDEN, "The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing", *International Data Privacy Law* 2011, à paraître.

placées dans le 'nuage' ne seraient pas nécessairement des données à caractère personnel dans le chef du fournisseur de service, par exemple lorsque ce dernier a pris le soin de les crypter de façon systématique, avant toute transmission, et pour autant que la technique de cryptage soit à l'épreuve des tentatives éventuelles de piratage. En outre, indépendamment du cryptage des données, le cloud computing présente cette particularité que les données accessibles à l'utilisateur au moyen de son compte d'accès ne sont pas nécessairement stockées en un lieu unique. Pour des raisons liées à la technique de stockage des informations, l'ensemble des données placées dans le 'nuage' font l'objet d'opérations de 'fragmentation', les différents 'fragments' étant conservés dans des espaces physiques différents. En d'autres termes, même si les données apparaissent à l'utilisateur comme figurant en un seul et même endroit, ceci ne correspond pas nécessairement au lieu de conservation physique des différents fragments. De la sorte, sauf à accéder par lui-même au compte de l'utilisateur, ce qui peut être interdit par contrat, le fournisseur de cloud computing ne serait pas en mesure, compte tenu des moyens dont il dispose, d'identifier les personnes concernées.

Ces chercheurs plaident aussi, *de lege ferenda*, pour une définition moins 'absolutiste' de la notion de données à caractère personnel, qui prenne dûment en compte les possibilités réelles d'identification d'une personne à l'aide des données mais aussi le risque objectif encouru. Cette proposition est faite dans le contexte de la révision annoncée de la directive 95/46, pour laquelle une proposition concrète de texte est en principe attendue de la Commission européenne pour la fin de l'année 2011.

Au plan des principes, nous pouvons souscrire en large partie à cette analyse. Nous pensons en effet que le but de la réglementation des données à caractère personnel est de protéger la vie privée et les autres droits et libertés fondamentales, et que pour cette raison, c'est en fonction de l'ensemble des circonstances de fait, notamment la nature des données et le degré de risques pour la vie privée, conformément au principe de proportionnalité, que l'on doit apprécier si et quelles données rendent une personne 'identifiable'[20]. Les réflexions sur le futur cadre réglementaire de la protection des données devraient, à notre avis, tenir compte du fait que la notion d'identité est plurielle et que 'l'identifiabilité' d'une personne est davantage une question d'échelle et de nuance, plutôt qu'un concept binaire.

Précisons néanmoins que la charte des droits fondamentaux de l'Union européenne[21] consacre désormais en son article 8 un "droit fondamental à la protection des données à caractère personnel"; ceci pourrait ouvrir la voie à des sanctions pour la violation des règles de protection des données, indépendamment de l'existence d'une atteinte, réelle ou supposée, grave ou légère, à la vie privée d'un individu[22].

21. Cela étant, ces considérations sur les techniques de cryptage et d'anonymisation, comme les contraintes techniques propres au cloud computing, ne sauraient à notre avis faire oublier au fournisseur de cloud computing ses responsabilités, dans le cas où il utiliserait, peu ou prou, les données stockées sur ses systèmes pour des finalités qui lui seraient propres. Elles ne font pas davantage échec aux obligations de sécurité et de confidentialité des données qui s'imposent non seulement au responsable du traitement, mais aussi, quoique indirectement, au sous-traitant choisi par ce dernier (voy. *infra*).

Et surtout, en pratique, l'entreprise qui collecte et traite des données personnelles pour les besoins de son activité aura, elle, du moins en principe, toujours accès à ses données, peu importe qu'elle les conserve sur un serveur en interne ou qu'elle les confie à un prestataire de cloud computing. Ainsi, il faut, nous semble-t-il, garder à l'esprit que les informations que l'utilisateur confie au 'nuage' n'en perdent pas, de ce fait, leur qualité de données à caractère personnel, à tout le moins dans le chef de cet utilisateur. Le fait même de recourir au cloud computing constitue d'ailleurs en soi un 'traitement', ou à tout le moins un moyen de ce traitement, au sens de la législation sur la protection des données. Et la personne qui détermine les moyens et les finalités d'un tel traitement reste, à n'en pas douter, pleinement redevable des obligations imposées par la loi du 8 décembre 1992.

2. Activités 'exclusivement personnelles et domestiques'

22. Une autre objection éventuelle à l'application de la loi du 8 décembre 1992 concerne plus spécifiquement les hypothèses où des personnes physiques utilisent des services et stockent des données sur Internet à des fins strictement personnelles.

En effet, de plus en plus de particuliers font confiance à un prestataire de cloud computing pour leur service de messagerie électronique personnelle, la gestion d'un répertoire d'adresses et de correspondants, la tenue d'une comptabilité privée, la sauvegarde et l'archivage de photos ou encore pour des applications bureautiques, etc. De telles activités nécessitent d'importants et nombreux traitements de don-

20. B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, pp. 88 et s., spéc. n° 165.

21. Charte des droits fondamentaux de l'Union européenne, adoptée le 7 décembre 2000 (*JOCE* 18 décembre 2000, C-364, pp. 1-22, vig. 1er janvier 2009). Le traité sur l'Union européenne dispose en son art. 6 que la Charte *"a la même valeur juridique que les traités"*.

22. B. DOCQUIR, *o.c.*, nos 140-145; voy. aussi deux décisions récentes de la Cour de justice de l'Union européenne: CJUE 29 juin 2010, C-28/08, *Commission / The Bavarian Lager*; 9 novembre 2010, aff. jointes C-92/09 et C-93/09, *Volker und Markus Schecke et Eifert*; voy. à ce sujet E. DEGRAVE, "Arrêt '*Volker und Markus Schecke et Eifert*': le droit fondamental à la protection des données à caractère personnel et la transparence administrative", *JDE* 2011, n° 178, p. 97.

nées personnelles. Or, la loi du 8 décembre 1992 et la directive 95/46 ne sont pas applicables aux traitements effectués par une personne physique *"pour l'exercice d'activités exclusivement personnelles ou domestiques"*[23]. On pourrait être tenté d'en déduire que tous les cas d'utilisation du cloud computing par une personne physique à des fins personnelles échapperaient à l'application de la loi du 8 décembre 1992.

En effet, des activités comme *"la correspondance et la tenue de répertoires d'adresses"* constituent bien des activités personnelles et domestiques; elles sont en tout cas expressément mentionnées comme exemples à ce titre par la directive 95/46[24].

23. Toutefois, l'exception relative aux activités exclusivement personnelles ou domestiques doit s'entendre dans un sens strict: elle vise uniquement les activités *"qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes"*[25]. Dans cette affaire, la Cour de justice connaissait à titre préjudiciel des activités d'une formatrice de catéchisme bénévole. Celle-ci avait créé un site web personnel, où elle avait publié des informations sur elle-même et ses collègues formateurs, lesquels se trouvaient identifiés par leurs nom et prénom, avec des indications sur leurs fonctions, leurs loisirs ou centres d'intérêt, et dans certains cas leur numéro de téléphone. Le site web en question était publiquement accessible, à un nombre indéterminé de personnes et sans limitation aucune, et il était référencé sur des sites tiers dont celui de l'Eglise de Suède. L'avocat général Tizzano, suivi par la Cour, avait alors rappelé, à juste titre, que l'exception liée aux activités personnelles et domestiques ne recouvrait que les seules activités *"manifestement privées et confidentielles, destinées à ne pas sortir de la sphère personnelle ou domestique des intéressés"*[26].

En d'autres termes, des activités consistant à traiter des données à caractère personnel sur un document édité à l'aide d'un traitement de texte ou d'un logiciel de messagerie disponibles en mode SaaS pourraient éventuellement être exclues du champ d'application de la loi du 8 décembre 1992, pour autant qu'elles relèvent strictement de la sphère personnelle de l'intéressé, et surtout à condition que ces documents ou ces données ne fassent pas l'objet d'une publication qui les rende accessibles à un nombre indéterminé de personnes.

24. Or, de nombreuses applications de cloud computing utilisées à des fins personnelles par des particuliers pour stocker des informations personnelles contiennent des outils dits de 'partage': pour ne prendre qu'un exemple, les outils de messagerie électronique sont de plus en plus étroitement intégrés aux sites de réseautage social, si bien qu'en un clin d'œil, un message, une image, une adresse Internet ou de courrier électronique figurant dans un courriel purement privé, peuvent se voir publiés sur le profil de l'utilisateur du réseau social, et être ainsi accessibles à un nombre plus ou moins important de personnes.

Entre la création d'un site web personnel comme celui de Mme Lindqvist, et l'activation de fonctions de publication ou de partage d'informations sur les réseaux sociaux, il n'y a sans doute pas la même implication personnelle ni la même conscience des conséquences possibles dans le chef de l'utilisateur. En droit, cependant, la frontière semble ténue, si bien que l'on peut penser qu'un clic de souris suffira parfois à entraîner l'application de la loi du 8 décembre 1992[27]. L'utilisateur particulier risque alors de ne pas pouvoir invoquer l'exception liée aux activités personnelles et domestiques[28], et pourrait se 'muer' en responsable du traitement, pour avoir ainsi publié des données à caractère personnel.

Quant au fournisseur de cloud computing, en fonction des circonstances de l'espèce, il pourrait lui aussi être qualifié de responsable du traitement, voire de coresponsable, ou de sous-traitant, au regard de la loi du 8 décembre 1992 (voy. *infra*). Mais dans le cas où les activités strictement personnelles et domestiques de ses clients viendraient à échapper à l'application de la loi du 8 décembre 1992, on peut se demander quelles règles encadreraient alors le traitement des données par ce prestataire. Ne serait-il pas souhaitable, dans ce cas, d'imposer au fournisseur de cloud computing certaines obligations minimales en termes de sécurité et de confidentialité, même en présence d'activités strictement personnelles et domestiques? Il est possible que cette question reçoive une réponse dans le contexte de la révision annoncée de la directive 95/46. A l'heure actuelle, toutefois, le fournisseur de cloud computing n'aurait, dans un tel cas, pas d'autres obligations de sécurité à assumer que celles qui résultent d'un éventuel engagement contractuel, pour autant bien entendu qu'il ne traite pas lui-même les données pour des finalités propres.

23. Art. 3, § 2 de la loi du 8 décembre 1992 et art. 3.2. de la directive 95/46.
24. Douzième considérant de la directive 95/46.
25. CJUE 6 novembre 2003, C-101/01, *Lindqvist / Suède*, par. 47.
26. Conclusions de l'avocat général Tizzano précédant l'arrêt du 6 novembre 2003, précité, par. 34.
27. Comme suggéré, à propos de la loi néerlandaise, par J.G.L. VAN DER WEES, "De verantwoordelijke en de verwerker in de cloud", *Computerrecht* 2011, liv. 64, p. 108.
28. Sauf, peut-être, à pouvoir démontrer que la publication n'était accessible qu'à un nombre limité de personnes, connues directement de l'intéressé. Voy. C. CUIJPERS, R. LEENES, S. OLIESLAEGERS et K. STUURMAN, *Rapport. De wolk in het onderwijs. Privacy aspecten bij cloud computing services*, SURFnet/Kennisnet Innovatieprogramma, disponible sur www.surfnetkennisnetproject.nl/innovatie/cloudcomputing/privacysecurity.

3. Champ d'application ratione loci

25. La nature intrinsèquement transfrontalière du cloud computing en fait un terrain d'élection naturel pour les questions relatives au domaine d'application territorial de la loi du 8 décembre 1992. Il convient toutefois de ne pas s'y tromper: ce n'est pas le lieu de stockage ou de conservation des données qui détermine l'application de la loi, mais bien le critère (principal) du lieu d'établissement du responsable du traitement, et éventuellement le critère (secondaire) du lieu où sont situés des '*moyens, automatisés ou non*', utilisés aux fins du traitement[29]. En principe, si le responsable est établi en Belgique[30], ou s'il recourt à des moyens de traitement situés sur ce territoire, la loi belge est applicable. Comme on va le constater, rares seront les hypothèses où l'on peut affirmer que tel n'est certainement pas le cas.

26. Dans le cadre de l'application du critère principal, les notions de lieu d'établissement et de responsable du traitement doivent évidemment être préalablement définies. Comme on le verra ci-après, l'identification du responsable du traitement n'est pas aisée dans un contexte de cloud computing, mais l'on peut en tout cas considérer que l'entreprise qui choisit d'externaliser son informatique sera très généralement qualifiée de responsable, sinon de coresponsable du traitement. L'établissement désigne *"l'exercice effectif et réel d'une activité au moyen d'une installation stable"*[31], en tenant compte non pas de la forme juridique, mais bien de l'affectation, en un lieu, de façon permanente ou en tout cas durable, de moyens humains et techniques nécessaires au traitement[32].

Par conséquent, la loi du 8 décembre 1992 s'appliquera chaque fois qu'une entreprise ou une organisation établie en Belgique recourt au cloud computing dans le cadre des activités réelles et effectives de cet établissement (soit dans la plupart des cas), même si le fournisseur de cloud computing est établi dans un autre Etat, et quel que soit le lieu où sont conservées les données.

De même, pour autant que le rôle du fournisseur s'apparente à celui d'un responsable ou d'un coresponsable du traitement, la loi sera également applicable, même si le client est établi hors de Belgique, dès lors que ledit traitement est effectué dans le cadre des activités d'un établissement fixe de ce fournisseur sur le territoire belge.

Il n'est pas aisé d'extrapoler ce raisonnement aux autres lois nationales transposant la directive 95/46, dans la mesure où la disposition de l'article 4 de cette directive a donné lieu à des régimes nationaux assez variés, l'harmonisation étant sur ce point assez peu poussée[33].

27. A l'image de la directive 95/46, la loi du 8 décembre 1992 possède un champ d'application 'extraterritorial', en vertu du critère secondaire d'applicabilité. Elle est en effet applicable dès lors que le responsable du traitement, établi par hypothèse hors de l'Union européenne, recourt à des moyens de traitement situés en Belgique, autres que ceux utilisés à des fins exclusives de transit sur le territoire belge.

Dans l'interprétation donnée à cette disposition par le groupe de l'article 29 et par plusieurs autorités nationales de protection des données, les fichiers dits *cookies* envoyés par un site web sur le disque dur des ordinateurs qui le 'visitent' constituent de tels 'moyens', à telle enseigne que pratiquement n'importe quel site web accessible en Belgique (et, par extension, en Europe), est susceptible d'être soumis à l'application de la loi du 8 décembre 1992 (et, par extension, des autres lois nationales transposant la directive 95/46[34]). Quels que soient les mérites de cette interprétation, elle paraît bien s'imposer dans plusieurs Etats membres, de sorte que l'on peut affirmer que pratiquement tout service de cloud computing est soumis à la loi du 8 décembre 1992 ou à une autre loi nationale transposant la directive 95/45, à raison soit des *cookies* placés sur l'ordinateur des personnes qui utilisent le service, soit encore d'autres moyens situés sur le territoire d'un Etat membre, tels qu'un ordinateur, un réseau de communications électroniques, un appareil permettant la connexion au réseau Internet, voire encore une simple interface graphique pour la connexion au service de cloud computing[35].

En d'autres termes, il paraît difficile d'échapper à l'application de la loi du 8 décembre 1992 *ratione loci*.

B. Répartition des rôles entre les différents intervenants et identification des personnes responsables

1. Présentation du problème

28. Comme on l'a vu, il est crucial d'identifier le responsable du traitement au sens de la réglementation sur la pro-

29. Art. 3*bis* loi 8 décembre 1992 et art. 4 dir. 95/46.
30. Plus précisément, si le traitement *"est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge (...)"*.
31. Considérant 19 de la directive 95/46.
32. C. CUIJPERS, "Toepasselijk privacyrecht in de wolk", *Computerrecht* 2011, liv. 64, p. 116 et note 14, et les références à la jurisprudence de la Cour de justice en matière d'établissement.
33. C. KUNER, *European Data Protection Law. Corporate Compliance and Regulation*, 2ème éd., Oxford University Press, 2007, pp. 117-118, n° 3.21. Pour un aperçu de la situation aux Pays-Bas, voy. C. CUIJPERS, "Toepasselijk privacyrecht in de wolk", *précité*.
34. Voy. les références citées par C. CUIJPERS, R. LEENES, S. OLIESLAEGERS et K. STUURMAN, *Rapport. De wolk in het onderwijs*, *précité*, p. 20 et note 33.
35. Voy. C. KUNER, *European Data Protection Law*, *précité*, pp. 118-128.

tection des données, parmi les différents acteurs d'un service de cloud computing. La répartition des rôles et les responsabilités des différents intervenants en découlent en effet directement.

29. Comme la directive 95/46, la loi du 8 décembre 1992 distingue et définit les rôles suivants[36]:

- le *responsable du traitement* est la personne physique ou morale, l'association de fait ou l'administration publique qui, *"seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement"*; le critère essentiel est celui du pouvoir de décision, qui incombe en principe à l'organe de gestion de la personne morale, sauf en cas d'association momentanée par exemple (association de fait); dans tous les cas, la responsabilité peut être conjointe, si les décisions concernant les moyens et les finalités du traitement sont prises de telle façon;
- le *sous-traitant* est *"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"*, c'est-à-dire en principe la personne qui traite les données pour le responsable, dans le cadre d'un mandat donné par ce dernier; le sous-traitant échappe à l'autorité directe du responsable, si bien que la notion ne recouvre pas la situation des employés et préposés du responsable;
- la *personne concernée* est la personne physique identifiée ou identifiable et concernée par une donnée à caractère personnel;
- le *tiers* est toute personne physique ou morale, toute association de fait ou toute administration publique, *"autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes placées sous l'autorité directe du responsable et habilitées à traiter les données"*, à savoir une personne physique ou morale étrangère à l'organisation du responsable du traitement; le tiers, aux yeux de la loi, est celui qui reçoit des données pour les utiliser *à des fins propres*; dès lors, les personnes qui sont sous l'autorité du responsable, de même que le sous-traitant, ne sont en principe jamais des tiers;
- le *destinataire* est toute personne physique ou morale, toute association de fait ou toute administration publique *"qui reçoit communication de données, qu'il s'agisse ou non d'un tiers"*; cette notion sert à identifier les flux de données, y compris les flux internes à l'organisation du responsable du traitement[37].

30. Ainsi que la doctrine l'a mis en évidence[38], le recours croissant aux technologies de l'information ne facilite pas l'interprétation des notions légales ni la répartition des rôles entre le responsable du traitement et le sous-traitant. En effet, il est de plus en plus fréquent que le fournisseur d'une infrastructure ou d'un logiciel, tout en se bornant à fournir un outil de traitement de l'information sans déterminer lui-même les finalités de ce traitement, prenne néanmoins un nombre important de décisions quant aux moyens dévolus à ce traitement[39]. L'observation est encore plus pertinente en cas d'externalisation, dès lors que le prestataire d'outsourcing est amené à prendre lui-même une série de décisions, tant en ce qui concerne les finalités que les moyens du traitement, même s'il agit pour le compte du client. Enfin, la question du partage des responsabilités est encore plus délicate dans un contexte où les fournisseurs qui mettent à disposition des clients leurs infrastructures, se réservent la possibilité de procéder eux-mêmes à d'autres traitements, pour des finalités propres, parfois même en agrégeant les données et en les rendant anonymes avant d'effectuer ce traitement.

31. Dans son avis 1/2010 sur les notions de 'responsable du traitement' et de 'sous-traitant'[40], le groupe de l'article 29 relève que la notion de responsable du traitement est une notion fonctionnelle, dépendante des circonstances de fait et visant à attribuer aux personnes qui exercent une influence de fait sur les données les responsabilités prévues par la loi. Elle nécessite donc une analyse factuelle plutôt que formelle. Les parties à un contrat ne sont ainsi pas entièrement libres de stipuler que l'une d'entre elles sera exclusivement considérée comme responsable du traitement. Une telle clause serait, à tout le moins, sans effet si elle ne correspondait pas à la réalité du pouvoir de décision sur les finalités et les moyens du traitement. Cela dit, le choix d'une stipulation contractuelle par les parties peut constituer une circonstance pertinente dans l'interprétation des faits et dans la recherche de la volonté commune des parties.

En pratique, il nous paraît vivement conseillé que les parties conviennent expressément de la répartition des rôles entre elles de ce point de vue, idéalement en précisant les limites de ce que chacune d'elles peut ou ne peut pas faire dans l'uti-

36. Art. 1er loi 8 décembre 1992; art. 2 dir. 95/46.

37. On notera que les autorités qui collectent des données dans le cadre d'une enquête fiscale, sociale ou judiciaire ne sont pas considérées comme des 'destinataires' aux yeux de la loi du 8 décembre 1992. Le responsable du traitement n'est donc pas tenu d'informer les personnes concernées en cas de transmission des données à de telles autorités.

38. T. LÉONARD et A. MENTION, "Transferts transfrontaliers de données: quelques considérations théoriques et pratiques" in B. DOCQUIR et A. PUTTEMANS (dir.), *Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, pp. 89-137.

39. Voy. aussi, à propos de la responsabilité des pouvoirs publics, E. DEGRAVE et Y. POULLET, "L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée", *JT* 2008, n° 6308, spéc. p. 283 et notes 64 et 65.

40. Groupe de travail 'Article 29' sur la protection des données, avis 1/2010 sur les notions de 'responsable du traitement' et de 'sous-traitant', WP 169, disponible sur http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2011_en.htm.

lisation des données personnelles. Le responsable du traitement a d'ailleurs l'obligation formelle de fixer, dans un contrat avec le sous-traitant, la responsabilité de ce dernier à son égard[41].

2. Interprétation des concepts selon le groupe de l'article 29

32. L'avis 1/2010 précité du groupe de l'article 29 a le mérite de préciser également que la détermination des moyens du traitement recouvre tant des questions techniques et organisationnelles, auxquelles les sous-traitants peuvent répondre eux-mêmes sans sortir de leur rôle, que des aspects essentiels du traitement, tels que les catégories de données qui sont traitées, les tiers qui y auront accès ou non, la durée de conservation, etc., soit 'le pourquoi et le comment'. Ainsi, la détermination des moyens n'impliquerait une responsabilité 'pleine' que si elle porte sur ces éléments essentiels, étant précisé par ailleurs que les moyens techniques et organisationnels ('non essentiels') peuvent être déterminés exclusivement par le sous-traitant.

33. Pour autant, l'action du sous-traitant doit rester dans les limites de la délégation qui lui est consentie par le responsable: s'il traite les données, c'est uniquement dans la mesure du mandat qui lui a été donné pour ce faire. Dès lors qu'il outrepasse ce mandat et acquiert un rôle propre dans la détermination des finalités ou des moyens essentiels du traitement, son rôle peut évoluer vers celui d'un coresponsable du même traitement, voire d'un responsable d'un autre traitement (selon le cas d'espèce).

34. Enfin, l'objectif de la réglementation étant de protéger les droits fondamentaux des individus à l'égard des traitements des données à caractère personnel les concernant, le recours à un sous-traitant, voire à une chaîne de sous-traitants successifs ou à un réseau de sous-traitants spécialisés dans différents aspects du traitement des données, devrait toujours être fait dans la transparence, le responsable du traitement étant toujours informé des principaux éléments de la structure de traitement: au plus le responsable est informé des subdélégations données par le sous-traitant, au plus il exerce une surveillance ou un contrôle sur l'exécution du service, et au plus il reste possible de considérer qu'il demeure, seul, le responsable du traitement au sens de la législation.

35. C'est, nous semble-t-il, au regard de ces quelques indications, qu'il convient d'apprécier les rôles respectifs de l'utilisateur du cloud computing et du (ou des) fournisseur(s). Il va sans dire qu'on aura égard au modèle de service en cause. Par exemple, la responsabilité du fournisseur d'une plate-forme PaaS ou IaaS sera, en règle, plus aisée à circonscrire et à cantonner dans les limites étroites que la loi assigne au rôle et à l'intervention du sous-traitant.

Il est par ailleurs important de préciser qu'une même entité peut être responsable à l'égard d'une activité ou d'un ensemble d'activités ou de traitements, et sous-traitant à l'égard d'une autre: en effet, la détermination des finalités et des moyens de chaque opération de traitement doit être évaluée distinctement, en relation avec le traitement concerné.

Quoique cela puisse sembler évident, précisons que le rôle d'un fournisseur de cloud computing doit naturellement s'apprécier non seulement à l'égard des données relatives à la personne même de son client ou du consommateur qui recourt à ses services, mais également vis-à-vis de l'ensemble des données à caractère personnel traitées à l'occasion de ce rapport contractuel avec un utilisateur: ce dernier peut en effet importer, collecter ou, plus largement, traiter des données relatives à un grand nombre de personnes, à commencer, par exemple, par sa clientèle, ses relations d'affaires, ses employés et ouvriers, etc.

3. Application aux plates-formes SaaS

36. Compte tenu de ce qui précède, il semble clair qu'en recourant à un service de type SaaS, l'utilisateur détermine les finalités et les moyens du traitement: c'est bien lui qui détermine pour quelles finalités les données seront traitées, quelles catégories de données seront traitées, quels droits d'accès les tiers auront sur ces données, quelle sera leur durée de conservation, etc.

Dans ce contexte, le fournisseur de cloud computing pourrait être considéré comme un simple sous-traitant, à condition qu'il n'accède pas de sa propre initiative aux données pour en faire un usage allant au-delà du mandat donné par le client.

Ainsi, certains fournisseurs de cloud computing annoncent ouvertement qu'ils peuvent faire usage de certaines données en propre, par exemple à des fins de marketing mais aussi à des fins de fourniture de services additionnels. Certains fournisseurs se réservent aussi la possibilité de communiquer les données à des tiers. Il va de soi que dans ces différentes hypothèses, le fournisseur de cloud computing sort de son rôle de simple sous-traitant pour assumer, en propre, des responsabilités dans la prise de décision non seulement quant aux moyens mais également quant aux finalités d'un autre traitement que celui correspondant à l'externalisation décidée par le client.

37. Pour autant, nous ne partageons pas l'opinion suivant laquelle, dans un grand nombre de cas, le fournisseur de solutions SaaS doit être considéré comme un coresponsable du traitement[42].

41. Art. 16, § 1er, 3° loi 8 décembre 1992.

42. J.G.L. VAN DER WEES, *précité*, invoquant notamment l'avis 10/2006 du groupe de l'art. 29 rendu à propos de l'affaire *Swift*.

Certes, ce fournisseur a bien la capacité de prendre des décisions propres à l'égard de certains traitements, et dans la pratique il prend effectivement un certain nombre de décisions concrètes concernant des aspects non négligeables des moyens du traitement, tels que la gestion de la sécurité, les copies de sauvegarde, le lieu de stockage des données et la fragmentation et la réplication de ces données.

Toutefois, s'il faut en croire l'avis 1/2010 du groupe de l'article 29, seule la délégation du pouvoir de décision sur des questions fondamentales pour la licéité du traitement est l'apanage du responsable du traitement. Ainsi, il se peut que l'éditeur d'un logiciel fourni en mode SaaS ait défini des options limitatives pour la sauvegarde des données ou la durée de conservation de celles-ci. En droit, néanmoins, cela n'enlève rien, selon nous, au pouvoir de décision du responsable du traitement qui recourt à cette application, et qui peut encore opter pour ces options limitatives en connaissance de cause, voire, le cas échéant, compléter les fonctions ou les services disponibles par un développement spécifique ou en recourant aux services d'un tiers.

38. A juste titre, l'avis 1/2010 précité indique : *"Le faible poids contractuel d'un petit responsable du traitement face à d'importants prestataires de services ne doit pas lui servir de justification pour accepter des clauses et conditions contractuelles contraires à la législation sur la protection des données."*

Il n'en reste pas moins vrai que les difficultés éventuelles qu'il y aurait à négocier certaines conditions contractuelles avec un fournisseur de cloud computing ne nous paraissent, en règle, pas pertinentes pour conférer à ce dernier une qualité de responsable du traitement, qui serait incongrue et incohérente au regard de son activité réelle quant aux données particulières d'un utilisateur.

Nous ne croyons pas, en effet, que l'on doive assimiler le développement et la configuration des logiciels ou des architectures d'information aux 'moyens du traitement' sur lesquels le responsable du traitement est en principe le seul à pouvoir prendre une décision. Il convient en effet de ne pas confondre les moyens du traitement, d'une part, et le service offert par un opérateur particulier, que le responsable du traitement sélectionne en connaissance de cause et après avoir examiné les fonctionnalités disponibles pour le traitement de l'information[43].

En tout état de cause, c'est bien entendu en fonction des particularités de chaque cas d'espèce qu'il conviendra de déterminer si l'utilisateur a décidé seul des finalités et des moyens 'essentiels' du traitement, ou si le fournisseur a endossé une responsabilité conjointe en allant au-delà de ses prérogatives de simple sous-traitant.

4. Application aux plates-formes PaaS et IaaS

39. Dans le contexte des plates-formes PaaS et IaaS, la possibilité pour le fournisseur de prendre des décisions autonomes sur les finalités et même sur les moyens du traitement des données paraît bien plus réduite encore. A notre avis, même si elle ne peut être exclue en fonction des circonstances de l'espèce, une qualification de responsable du traitement semble dès lors improbable.

Des auteurs anglais s'interrogent d'ailleurs, à titre prospectif, sur la possibilité d'exclure même la qualification de sous-traitant dans le chef d'un certain nombre de fournisseurs de cloud computing. D'après eux, on ne devrait pas qualifier de sous-traitants des opérateurs qui se limitent à fournir des capacités de calcul et de stockage de données, sans aucune possibilité d'en prendre connaissance ni d'en faire quelque usage que ce soit, en particulier s'agissant de données cryptées, et lorsque des garanties contractuelles, techniques et organisationnelles solides tendent à empêcher radicalement tout usage de et tout accès aux données dans le chef de ces opérateurs. Ces auteurs appellent de leurs vœux une clarification des notions de responsable du traitement et de sous-traitant dans la législation sur la protection des données, mais également la consécration, au bénéfice de ces fournisseurs, 'intermédiaires techniques', d'un régime de responsabilité allégée, voire d'une exemption limitée de responsabilité, à la manière de celle consacrée par la directive 2000/31/CE sur le commerce électronique en faveur de certains intermédiaires de l'Internet[44].

C. Aperçu des principaux aspects de la réglementation des données personnelles

40. Une fois résolues les délicates questions du champ d'application de la loi et de l'identification du ou des responsables, nous pouvons passer à un (très bref) aperçu du régime de la protection des données. Nous serons volontairement succincts, puisque les règles exposées ci-après ne suscitent pas de difficultés d'application spécifiques dans le contexte du cloud computing, sous réserve de la question des transferts de données dans d'autres pays[45]. Pour la clarté de l'exposé, et parce que nous pensons que cela correspond à une réalité pratique dans de nombreux cas, nous partirons de l'hypothèse que l'entreprise utilisatrice du cloud computing

43. Dans le même sens, à propos des marchés publics, voy. E. DEGRAVE et Y. POULLET, *o.c.*, p. 283.

44. Voy. W. K. HUON, C. MILLARD et I. WALDEN, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2", *Legal Studies Research Paper*, n° 77/2011, Queen Mary University of London, School of Law, accessible via http://papers.ssrn.com/sol3/Display-AbstractSearch.cfm.

45. Pour plus de détails sur le régime de la loi du 8 décembre 1992 en général, voy. notamment T. LÉONARD, "La protection des données à caractère personnel et l'entreprise", *Guide juridique de l'entreprise*, Kluwer, 2004; B. DOCQUIR, *Le droit de la vie privée*, *o.c.*; D. DE BOT, *Verwerking van persoonsgegevens*, Kluwer, 2001.

est le responsable du traitement, tandis que le fournisseur de cloud computing est le sous-traitant.

1. Les règles fondamentales

41. Mentionnons d'abord, presque pour mémoire, les règles fondamentales consacrées aux articles 4 et 5 de la loi du 8 décembre 1992.

Tout traitement de données doit être effectué loyalement et licitement, pour des finalités déterminées, explicites et légitimes, en se limitant à des données adéquates, pertinentes et non excessives au regard des finalités poursuivies, en veillant au caractère exact et à la mise à jour des données, et en ne conservant ces dernières que pendant le temps nécessaire à la réalisation du ou des buts poursuivis.

Si l'entreprise souhaite traiter les données ultérieurement, pour des finalités autres que celles applicables lors de l'obtention des données, cela suppose que les 'nouvelles' finalités soient compatibles avec les premières, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. Les traitements ultérieurs à des fins historiques, scientifiques ou statistiques doivent par ailleurs être effectués dans le respect des dispositions de l'arrêté royal du 13 février 2001 (précité).

Tout traitement doit, en outre, reposer sur l'une des bases légales énumérées à l'article 5 de la loi. Dans le cas d'une entreprise, il s'agira le plus souvent soit du consentement des personnes, soit de la poursuite de l'intérêt légitime de l'entreprise dans le respect du principe de proportionnalité, soit encore de l'exécution d'un contrat auquel la personne concernée est partie; en cas de mesures d'investigation par les autorités policières ou judiciaires, l'entreprise pourra invoquer le cas du traitement *"nécessaire au respect d'une obligation légale du responsable du traitement"*, visé à l'article 5, c) de la loi du 8 décembre 1992.

42. Le responsable du traitement doit informer les personnes concernées et se montrer transparent en ce qui concerne les données et le traitement qui leur est réservé. Il doit effectuer une déclaration auprès de la Commission de la protection de la vie privée, conformément à l'article 17 de la loi, et communiquer individuellement à toutes les personnes concernées les informations visées à l'article 9 de la loi.

Les personnes concernées disposent toujours du droit de s'opposer, gratuitement et sans justification, à l'utilisation de leurs données à des fins de marketing direct. Elles disposent aussi du droit d'accéder aux données les concernant et d'obtenir des informations sur le traitement, ainsi que du droit de faire rectifier des données inexactes ou incomplètes, et de faire mettre fin au traitement de toute donnée incomplète, non pertinente, communiquée de façon illicite à un tiers ou conservée au-delà de la période autorisée.

43. Enfin, le responsable du traitement doit assurer la sécurité et la confidentialité des données, conformément à l'article 16 de la loi. Il doit, notamment, choisir un sous-traitant présentant des garanties suffisantes au regard des mesures de sécurité techniques et organisationnelles relatives au traitement. Nous abordons ces questions ci-après, à propos de la relation contractuelle avec le sous-traitant.

2. Les données sensibles

44. Si des données sensibles ou des données relatives à la santé sont traitées dans le cadre des services de cloud computing utilisés par l'entreprise, celle-ci est tenue par les règles particulières énoncées aux articles 6 et 7 de la loi du 8 décembre 1992. En substance, le traitement de telles données est interdit, sauf à disposer du consentement écrit des intéressés, ou dans certaines autres hypothèses strictement et limitativement définies par la loi.

En vertu de la loi, le Roi a précisé et renforcé les obligations du responsable de veiller à la sécurité des données sensibles et des données relatives à la santé[46]. Nous ne citerons ici que l'obligation de désigner les catégories de personnes qui ont accès aux données et de veiller à ce qu'elles soient tenues par une obligation de confidentialité.

Signalons aussi qu'en matière de données relatives à la santé, la loi impose l'intervention d'un professionnel des soins de santé, sauf lorsque le traitement a reçu l'accord écrit de l'intéressé.

45. Indépendamment des règles propres à la loi du 8 décembre 1992, il va de soi que des réglementations particulières peuvent s'appliquer aux différentes catégories de données susceptibles d'être traitées dans un contexte de cloud computing. Nous pensons ainsi à toutes les obligations légales ou réglementaires de conserver certaines archives sur le territoire du Royaume ou à tout le moins de permettre à l'administration d'y accéder aisément en cas de contrôle. Nous songeons également aux dispositions de la législation hospitalière qui imposent de conserver les données du patient à l'hôpital.

3. Les transferts de données dans et hors de l'Union européenne

46. On sait que l'un des objectifs de la directive 95/46 est d'assurer la libre circulation des données à caractère personnel au sein de l'Union européenne (et de l'Espace économique européen). Par conséquent, le transfert de données de Belgique vers d'autres Etats membres n'est en principe soumis à aucune autorisation ni restriction.

46. Voy. les art. 25, 26 et 27 de l'AR du 13 février 2001, *précité*.

En revanche, les transferts vers des pays hors de l'Union européenne ne sont autorisés que moyennant des conditions assez sévères[47].

En pratique, un tel transfert ne pourra le plus souvent avoir lieu que vers un des quelques pays identifiés par la Commission européenne comme présentant un niveau de protection adéquat, ou bien par le recours à l'une des méthodes de transfert spécifiques mises sur pied par la Commission (règles contraignantes d'entreprise, clauses types, *Safe Harbor*, etc.)[48].

47. Le régime des transferts de données est-il applicable dans un contexte de cloud computing? La réponse paraît immanquablement positive, puisqu'à première vue les centres de données des fournisseurs sont situés un peu partout dans le monde, et qu'aussi bien les données 'voyagent' d'un centre de données à l'autre pour des raisons de stockage et de bon fonctionnement du service.

La question mérite toutefois d'être approfondie, au regard de l'arrêt du 6 novembre 2003 de la Cour de justice de l'Union européenne, déjà examiné ci-avant. L'une des questions posées à la Cour portait sur l'application du régime de transfert de données personnelles vers des pays tiers à l'Union européenne. Dans son arrêt, la Cour juge que lorsqu'une personne établie sur un Etat membre inscrit sur une page Internet, stockée auprès de son fournisseur de services d'hébergement établi dans ce même Etat membre ou dans un autre Etat membre, des données à caractère personnel, il n'existe pas de 'transfert' au sens de l'article 25 de la directive 95/46[49].

Nonobstant cette décision, la plupart des commentateurs considèrent que lorsque des données personnelles sont mises à disposition sur un serveur, dans le but d'être transmises à des destinataires ou à des tiers, l'on est bien en présence d'un transfert de données soumis au régime spécifique des articles 25 et 26 de la directive 95/46[50].

En effet, la *ratio legis* de ce régime particulier est de protéger la vie privée des intéressés chaque fois qu'un responsable de traitement communique des données à un tiers situé dans un Etat non membre de l'Union européenne, dans le but de soumettre ou de faire soumettre ces données à un traitement dans ce dernier pays.

48. L'autorité danoise de protection des données a dû se prononcer sur le recours par une municipalité à la suite bureautique en ligne 'Google Apps', à travers la conclusion d'un contrat avec la société de droit irlandais Google Ireland Ltd, prévoyant l'hébergement des données dans les *data centers* de la société de droit américain Google Inc[51]. L'autorité danoise a estimé que le transfert des données vers les *data centers* de Google Inc. situés aux Etats-Unis était admissible, compte tenu de l'adhésion de cette société aux principes du *Safe Harbour*. En revanche, elle a estimé que le transfert vers des *data centers* situés dans d'autres pays, non membres de l'Espace économique européen, ne pouvait, en règle, pas être admis, à défaut de démontrer que de tels pays présentent un niveau de sécurité adéquat. Or, Google avait explicitement annoncé que les données seraient stockées sur des *data centers* situés dans le monde entier, plutôt que d'être placées sur un serveur ou un ensemble de serveurs déterminés.

49. C'est pourquoi une solution pragmatique consiste à obtenir du fournisseur l'engagement contractuel que les données ne quitteront pas le territoire de l'Union européenne (ou de l'Espace économique européen), par la sélection du ou des *data centers* sur lesquels les données seront hébergées. L'idéal est en fait de viser expressément le territoire des Etats membres de l'Espace économique européen, et de stipuler un engagement contractuel du fournisseur que les données ne quitteront pas le territoire de ces Etats.

IV. PROTECTION DES DONNÉES: LA RELATION CONTRACTUELLE ENTRE LE FOURNISSEUR ET L'UTILISATEUR, PIERRE ANGULAIRE DU RESPECT DES RÈGLES DE PROTECTION DES DONNÉES DANS LE CONTEXTE DU CLOUD COMPUTING

A. Obligations de sécurité et de contrôle incombant au responsable du traitement

50. Comme évoqué ci-avant, le responsable du traitement doit assumer diverses obligations liées à la sécurité des données et à l'organisation et au contrôle des accès et des usages des données par ses employés et préposés, mais aussi par son ou ses sous-traitants. Ces obligations sont énumérées à l'article 16 de la loi du 8 décembre 1992.

Tout d'abord, le responsable doit prendre les mesures techniques et organisationnelles requises pour protéger les données contre les risques d'atteintes et de traitements illicites. Ces mesures doivent être établies en tenant compte de la

47. Art. 21 et 22 loi 8 décembre 1992 et art. 25 et 26 dir. 95/46.
48. Pour plus de détails, voy. C. KUNER, *European Data Protection Law*, *précité*, chapitre 4, ainsi que T. LÉONARD et A. MENTION, "Transferts transfrontaliers (…)" in B. DOCQUIR et A. PUTTEMANS (dir.), *Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, pp. 89-137.
49. CJUE 6 novembre 2003, C-101/01, *Lindqvist / Suède*, par. 71.
50. C. KUNER, *European Data Protection Law*, *o.c.*, n° 4.08; T. LÉONARD et A. MENTION, "Transferts transfrontaliers (…)" in B. DOCQUIR et A. PUTTEMANS (dirs.), *Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, pp. 89-137.
51. La decision, traduite en anglais, est disponible sur le site www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

nature des données, des risques encourus pour les personnes concernées, de l'état de la technique et du coût des mesures envisagées.

Ensuite, le responsable doit s'assurer que les programmes servant au traitement des données soient conformes aux termes de la déclaration faite auprès de la Commission de la protection de la vie privée et qu'il n'en est pas fait d'usage illicite.

En outre, le responsable doit communiquer des instructions à ses préposés et leur imposer une obligation de confidentialité.

Le responsable du traitement doit encore limiter l'accès des personnes placées sous son autorité aux données à caractère personnel, et s'assurer ainsi que seuls ceux qui en ont réellement besoin pour l'exercice de leurs fonctions puissent avoir accès aux données et les utiliser, dans les limites des données qui sont strictement nécessaires à cette fin.

Pour terminer, le responsable doit encore former et sensibiliser ses préposés à la politique de sécurité mise en place au sein de l'entreprise.

B. Rapports entre le responsable et le sous-traitant

51. Par ailleurs, la loi encadre étroitement les rapports entre le responsable du traitement, d'une part, et le ou les sous-traitants, d'autre part.

Ainsi, le responsable doit choisir un sous-traitant offrant des garanties suffisantes au regard des mesures de sécurité qu'il a définies. Il doit donc lui décrire ces mesures, idéalement par écrit, préalablement à la conclusion du contrat. Il peut également s'avérer utile de faire dresser par le candidat sous-traitant l'inventaire des mesures de sécurité qu'il s'engage à observer en cas de conclusion du contrat de sous-traitance.

De même, le responsable doit s'assurer que le sous-traitant retenu respecte bien les mesures de sécurité, et ce *"notamment par la stipulation de mesures contractuelles"*. Ici aussi, annexer au contrat de sous-traitance la politique de sécurité, pourra contribuer à l'aménagement de la preuve et faciliter quelque peu la tâche de l'utilisateur en cas de litige.

Enfin, et surtout, le responsable du traitement doit établir un contrat écrit avec le sous-traitant, dans lequel il doit stipuler que le sous-traitant ne peut traiter les données que sur ses instructions, et fixer la responsabilité du sous-traitant envers lui.

C. Aspects pratiques de la relation avec le sous-traitant

52. Une étude intéressante a mis en évidence une grande diversité dans la fixation des responsabilités respectives de l'utilisateur et du fournisseur au sein des conditions générales d'utilisation de différents fournisseurs de cloud computing (SaaS, PaaS et IaaS)[52]. Il est donc important d'analyser soigneusement les conditions proposées sous l'angle de la protection des données, au regard des indications rappelées ci-avant.

Il va de soi, du reste, que le fournisseur de cloud computing aura tendance à rechercher la plus grande standardisation possible dans les relations contractuelles avec ses clients. Ainsi, il souhaitera légitimement définir lui-même les règles de sécurité des données. Une telle approche n'est pas nécesairement incompatible avec les règles de protection des données, à condition toutefois que le responsable du traitement ait effectivement pu vérifier au préalable que ces règles lui donnent satisfaction, et que l'accord entre les parties soit clair et transparent.

53. La décision précitée de l'autorité danoise de protection des données illustre à quel point certains services actuellement disponibles sur le marché sont défaillants au regard du niveau d'exigence de la directive 95/46 en ce qui concerne les relations entre le responsable et le sous-traitant.

Ainsi, l'autorité danoise de protection des données relève notamment que le contrat standard relatif au service 'Google Apps' ne répond pas aux exigences légales concernant la relation entre la municipalité responsable du traitement et le sous-traitant. En effet, ce contrat standard ne stipule pas que Google Ireland Ltd s'engage à ne traiter les données que sur les instructions de la municipalité. De plus, il n'est pas exclu que ce contrat soit modifié unilatéralement par Google. En outre, ce contrat ne contient aucune référence à des obligations de sécurité pourtant imposées à Google en vertu du droit danois. L'autorité danoise s'interroge également sur la possibilité concrète pour la municipalité de contrôler les traitements effectués par Google, dès lors qu'elle ignore où les données se trouvent exactement.

54. Ceci démontre que le responsable du traitement doit prendre des initiatives et imposer des exigences concrètes à son fournisseur, s'il veut agir dans le respect de la loi du 8 décembre 1992.

Ainsi, non seulement la conclusion d'un contrat entre l'utilisateur et le fournisseur de cloud computing est obligatoire, mais en outre les parties doivent apporter le plus grand soin à la rédaction de ce contrat. En particulier, celui-ci doit impérativement régler la responsabilité respective du sous-trai-

52. S. BRADSHAW, C. MILLARD et I. WALDEN, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", *Legal Studies Research Paper*, n° 63/2010, Queen Mary University of London, School of Law, accessible via http://papers.ssrn.com/sol3/DisplayAbstractSearch.cfm.

tant et du responsable du traitement, la question de l'accès aux données, l'interdiction faite au fournisseur de cloud computing de traiter les données pour des fins propres, etc.

55. Plus largement, au vu des exigences qui pèsent sur le responsable du traitement, nous pensons que c'est l'ensemble de la politique de sécurité et de protection des données de ce dernier qui devrait être transposée et reflétée dans l'accord conclu avec le fournisseur de cloud computing. En effet, ce n'est pas parce que l'entreprise externalise ses données qu'elle peut entièrement déléguer ses obligations en termes de sécurité.

Ainsi, le premier devoir du responsable du traitement est de prendre des mesures de sécurité. Il va de soi que l'utilisateur qui confierait ses données à un fournisseur de cloud computing sans interroger ce dernier sur les mesures de sécurité qu'il met en place, et sans imposer d'exigences minimales à cet égard, manquerait à ses obligations en tant que responsable de traitement.

56. Au-delà de cet exemple évident, l'on retiendra que le recours à l'informatique dématérialisée ne peut se faire sans une réflexion approfondie du responsable du traitement sur les aspects techniques de l'externalisation et sur le niveau de sécurité à atteindre dans la collaboration avec le fournisseur.

Concrètement, il nous paraît que le contrat avec le sous-traitant doit rencontrer à tout le moins les préoccupations suivantes.

D'abord, les mesures de sécurité doivent être incorporées au contrat avec le sous-traitant, fût-ce par référence, et le responsable doit disposer des moyens de contraindre le fournisseur à exécuter ces mesures. Il convient, à cet égard, de tenir compte des particularités du contexte du cloud computing, notamment du fait que les données sont susceptibles d'être stockées dans un environnement distribué (nombreux *data centers*), ou encore du fait que les données seront stockées sur des serveurs qui accueillent aussi les données de tiers. Les mesures de sécurité doivent en effet être adaptées aux circonstances, comme le veut la loi.

En outre, le fournisseur doit se voir interdire de traiter les données au-delà ou en l'absence d'instructions précises du responsable du traitement. Si tel n'est pas le cas, du moins convient-il de préciser dans quels cas, avec quelles données et dans quels buts le fournisseur se réserve d'effectuer de tels traitements propres.

Enfin, il nous semble que le responsable du traitement doit avoir la possibilité concrète et effective de 'revenir en arrière', et de récupérer la maîtrise de ses données, selon des modalités pratiques, techniques et financières que les parties auront avantage à régler lors de la conclusion du contrat.

57. L'on ne saurait par ailleurs trop conseiller aux entreprises et organisations qui souhaitent recourir au cloud computing, comme aux fournisseurs de cloud computing, non seulement de stipuler clairement par écrit leurs responsabilités respectives à cet égard, mais aussi de promouvoir autant que possible la transparence dans le traitement des données.

Ceci concerne en particulier l'implication éventuelle de tiers qui fourniraient des services par l'intermédiaire de la plate-forme PaaS ou qui seraient sous-traitants d'un intégrateur sur une plate-forme IaaS. En effet, dans une telle hypothèse (pluralité de sous-traitants), selon l'avis 1/2010 précité du groupe de l'article 29, l'utilisateur du cloud computing ne pourrait être qualifié de seul et unique responsable du traitement qu'en prenant en considération une série de critères tels que, notamment, le niveau de précision et la quantité d'instructions données par le responsable au sous-traitant principal, la surveillance exercée par lui sur l'exécution du service, les attentes suscitées dans le chef des personnes concernées au vu de l'image donnée par le responsable du traitement et, enfin, le niveau d'expertise particulier du prestataire de services. Si ces différentes questions sont abordées dans le contrat et si les parties définissent avec précision leurs droits et obligations respectifs concernant chacune d'elles, cela permettra sans doute de faire la lumière nécessaire sur les responsabilités respectives de l'utilisateur et des divers fournisseurs de logiciels, de plates-formes et d'infrastructures du cloud computing, au regard de la loi du 8 décembre 1992.

58. La conclusion d'un accord entre le responsable et le sous-traitant s'avère aussi utile, voire indispensable, pour assurer le respect effectif des droits des personnes concernées. Ainsi, si c'est le sous-traitant qui est en contact avec les intéressés, c'est lui qui, dans la pratique, sera saisi des demandes d'accès, de rectification ou d'opposition. Il est dès lors préférable de stipuler dans le contrat l'obligation du sous-traitant d'agir promptement pour communiquer les demandes des particuliers fondées sur l'un de ces droits. Ainsi encore, il se peut que le fournisseur de cloud computing soit mieux placé que l'utilisateur pour communiquer aux personnes concernées les éléments d'information obligatoires visés à l'article 9 de la loi. Dans ces cas, le contrat de cloud computing devrait clairement stipuler les modalités de collaboration entre parties pour réagir aux diverses demandes des personnes concernées.

59. Dans la pratique, de tels conseils trouveront sans doute un écho favorable lorsque les données sont jugées importantes ou stratégiques par l'entreprise elle-même, mais les règles de protection des données s'appliquent à toutes les catégories de données à caractère personnel, indépendamment de leur importance ou de leur valeur pour le responsable du traitement.

C'est en ce sens que nous croyons pouvoir dire que dans le contexte du cloud computing, les exigences de la protection des données rejoignent l'intérêt bien compris de l'entreprise qui recourt à l'informatique dématérialisée: plutôt que

comme des contraintes, elles devraient donc être vues comme un atout, permettant de négocier au mieux le contrat avec le fournisseur en attirant l'attention sur des points auxquels les parties ne songent pas nécessairement au moment de la conclusion du contrat, dans l'euphorie d'une collaboration prometteuse et des substantielles économies qui sont annoncées. Quant au fournisseur, il a, lui aussi, un intérêt certain à offrir à ses clients un service qui, sur le long terme, ne risque pas d'être remis en cause pour des motifs tenant aux règles de protection des données.