DOCTRINE

Cloud computing et protection des données à caractère personnel : mise en ménage possible ? [1]

Jean-Marc Van Gyseghem[2,3]

Le cloud computing *soulève bon nombre de questions qui, si elles ne sont pas nouvelles, exacerbent certaines problématiques déjà existantes. Le* cloud computing *impose donc des réflexions qui constituent un challenge pour les juristes.*
La présente contribution s'attache plus particulièrement à des aspects propres au domaine de la protection des données à caractère personnel. À défaut de pouvoir les aborder tous, nous avons limité notre propos aux questions de détermination des responsables de traitement et sous-traitants ainsi qu'aux principes d'information, de confidentialité et de sécurité.

L'angle pris est celui par rapport à une P.M.E. ou à un indépendant utilisant le cloud computing *dans le cadre de ses activités professionnelles/commerciales.*

• • •

Cloud computing is not a new concept from the point of view of technology but raises several issues which were already existing. It builds a new challenge for the lawyers.
This paper explores issues related to data protection. Unfortunately, we cannot go through all of them and we have to select them. Therefore, we'll give an approach to the determination of data controller and data processor as well as the concepts of information, confidentiality and security.

We tackle these issues thru the prism of SME and self-employed person using the cloud computing in its commercial or professional activities.

1 L'auteur renvoie le lecteur à diverses contributions relatives au *cloud computing* et à la vie privée telles que, sans exhaustivité, S. Bradshaw, *Cloud Computing CCLS Cloud Legal Research Project* ; S. Bradshaw, *Presentation on Cloud Computing : Security and Privacy Aspects and Cloud Contracts*, Ankara, May 2010 ; S. D.J. Solove, « I've got nothing to hide and other misunderstandings of privacy », *San Diego Law Review*, Vol. 44, 2007 ; GWU Law School Public Law Research Paper No. 289 ; R. Clarke et D. Stavensson, « Privacy and Consumers Risks in Cloud Computing », in *Computer Law and Security Review*, 2010, Vol. 26 n° 4, pp. 391-397.

2 Avocat au barreau de Bruxelles et directeur de l'Unité « Libertés dans la société de l'information » du Centre de Recherches Informatique et Droit de la Faculté de Droit de Namur (CRIDS).

3 Le présent article ne reflète que les opinions personnelles de l'auteur. Il remercie cependant les membres du CRIDS pour les discussions fructueuses relatives au *cloud computing*.

1. Le *cloud computing* est un phénomène (de mode ?) qui prend une place de plus en plus importante dans les nouvelles technologies au point que l'internaute en use (et abuse ?) sans réellement s'en rendre compte. Ainsi, il en va pour Facebook, gmail, doodle, Office 365, etc.

Il s'agit également d'un phénomène qui se vend. Certains fournisseurs de produits informatiques n'hésitent donc pas à offrir un service/produit comme étant du *cloud computing* alors qu'il ne s'agit, en réalité, que de la mise en place d'un réseau domestique.

Le *cloud computing* a ceci de particulier qu'il semble faire revenir en arrière la maîtrise des personnes sur leurs données dès lors qu'elles s'en dessaisissent à l'instar d'il y a 20 ans lorsque les ordinateurs n'étaient, en réalité, que des terminaux raccordés à de gros serveurs centralisés. Ces terminaux ne contenaient aucune donnée à l'instar de la situation actuelle avec le *cloud computing*. N'est-ce pas paradoxal ? À noter également que même des juristes soucieux des questions de protection des données à caractère personnel utilisent le *cloud computing* pour leur messagerie…

2. Le *cloud computing* soulève un certain nombre de questions à tous niveaux (*law enforcement, data retention*, etc.), mais toutes ne pourront être analysées dans le cadre de la présente contribution.

L'on doit cependant relever, et nous le verrons plus loin, que le *cloud computing* ne soulève pas nécessairement de nouvelles questions mais les pousse beaucoup plus loin et toutes en même temps. C'est en cela que le *cloud computing* constitue un véritable challenge pour les juristes et, plus particulièrement, ceux qui traitent de la protection des données à caractère personnel.

L'on doit donc être attentif à cet élément qui permet de placer le *cloud computing* dans sa vraie perspective.

3. Dans le cadre de la présente contribution, nous aborderons le *cloud computing* sous l'angle des personnes morales ou des travailleurs indépendants l'utilisant dans l'exercice de leurs activités commerciales professionnelles. Manifestement, les personnes morales ou travailleurs indépendants traitent des données à caractère personnel que ce soient celles, par exemple, de leurs employés ou celles de leurs clients/fournisseurs.

Ils sont, par ailleurs, souvent confrontés à des questions de coût des services et matériels IT et donc tentés de faire appel au *cloud computing* pour externaliser une partie de leur infrastructure IT avec un service de maintenance associé et fourni par le fournisseur de *cloud computing*.

Nous devons donc analyser le rôle qu'endossent ces personnes au sens 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 (loi Vie privée) avec les implications que cela engendre.

Dans le cadre de la présente contribution, nous parlerons d'utilisateur pour désigner la personne morale ou le travailleur indépendant utilisant le *cloud computing* dans l'exercice de son activité commerciale professionnelle et le fournisseur de *cloud computing* sera désigné par l'acronyme CCP (*cloud computing provider*).

4. On se permet cependant d'analyser brièvement la question de l'exception d'applicabilité de la loi Vie privée qui prévoit une exception majeure à son application dès lors que les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques sont exclus du champ d'application de la loi.

L'on doit, bien évidemment, prendre en compte cette exception lorsque l'on traite du *cloud computing* puisque bon nombre de personnes physiques l'utilisent pour des traitements qui sont effectués à des fins exclusivement

personnelles ou domestiques. Pensons, ainsi, aux services de messagerie ou de bureautique proposés par les grands acteurs informatiques tels que Microsoft (Office 365) ou Google (gmail, Google document) qui sont utilisés par des particuliers.

Cela signifie que des personnes physiques dont leurs données à caractère personnel sont traitées dans ce cadre-là ne pourront pas bénéficier de la protection de la loi alors même que de telles données circulent à travers le *cloud* avec l'insécurité que cela peut générer. Ce sentiment d'insécurité est d'autant plus présent que les contrats conclus sont essentiellement des contrats d'adhésion sans aucune possibilité de négociation de la part du particulier qui est manifestement une personne faible dans la transaction. Peut-on réellement imaginer un particulier négocier son contrat avec un des gros acteurs informatiques ? La réponse est bien entendu négative.

Cette exception peut, bien évidemment, être source de discrimination entre des personnes qui voient leurs données traitées soit dans le cadre d'activités domestiques d'une personne physique, soit dans celle de cette même personne physique mais dans une activité professionnelle.

Ne doit-on pas s'interroger sur la pertinence d'une telle exception alors qu'il existe un réel risque de perte de contrôle de ces données tant par celui qui les traite que la personne dont les données sont traitées ? À l'heure actuelle et compte tenu de la rédaction tant de la directive 95/46 que de la loi Vie privée, cette exception est présente et on doit en tenir compte dans l'approche du *cloud computing*.

I. INTRODUCTION

5. D'entrée de jeux, il nous faut impérativement planter le décor afin que l'on puisse ensuite y faire jouer les acteurs.

Nous ne ferons pas œuvre de grande originalité en vous proposant, comme définition du *cloud computing*, celle donnée par le National Institute of Standards and Technology (NIST) qui semble le mieux résumer ce qu'il est. Nul besoin de « réinventer la roue » tant la définition est, à ce jour, représentative de la notion même du *cloud computing* :

> *« Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential* ***characteristics****, three* ***service models****, and four* ***deployment models****. »*[4]

Cette définition donne un certain nombre de caractéristiques que le NIST qualifie d'essentielles[5] :

– *Un self-service rapide et élastique sur demande :* de manière automatique et sans aucune intervention humaine, l'utilisateur peut augmenter les capacités du service offert. Il peut ainsi augmenter l'espace mémoire disponible, le type de service souhaité, etc.

– *Un large accès :* l'utilisateur peut accéder au *cloud computing* par l'intermédiaire

[4] P. Mell et T. Grance, « The NIST Definition of Cloud Computing », version 15, 10 juillet 2009, available at http://csrc.nist.gov/groups/SNS/cloud-computing/.

[5] P. Mell et T. Grance, « The NIST Definition of Cloud Computing », version 15, 10 juillet 2009, available at http://csrc.nist.gov/groups/SNS/cloud-computing/.

de tout type de réseau et de terminal, la seule exigence est qu'il soit connecté à Internet.

– *Un centre de ressources :* le CCP offre une série de services pouvant aller du stockage au logiciel de courriers électroniques ; services qui peuvent être « actionnés » par l'utilisateur à tout moment.

– *Un service sous contrôle :* le CCP peut contrôler et optimiser les ressources utilisées. Cela implique que les données d'une même personne, qu'elle soit physique ou morale, peuvent être « éclatées » entre divers lieux d'hébergement pour des questions d'optimalisation des ressources.

Ces caractéristiques sont commercialement intéressantes et attirantes mais cachent, bien évidemment, des aspects qui atténuent – dans un certain sens – le côté idéal du *cloud computing* :

– Le problème posé par la nécessité d'avoir un accès Internet. En effet, l'utilisateur ne pourra pas accéder aux services du *cloud computing* et se trouvera donc totalement démuni sans cet accès. Si, pour un « simple » particulier, cela n'a guère d'importance hormis une certaine frustration, il n'en va pas de même pour une administration ou tout autre personne – morale ou physique – qui doit assurer une continuité de service. Cela pourrait engager la responsabilité de la personne qui est dans l'incapacité de rendre le service demandé pour une question de connexion à Internet défaillante. On pourrait, en effet, lui reprocher d'avoir opté pour une solution qui ne garantisse pas la continuité de service à laquelle il s'est engagé légalement ou contractuellement quitte à ce qu'elle exerce une action en garantie à l'encontre du fournisseur Internet (ISP). Elle restera cependant le premier responsable pour le créancier du service.

– Le caractère élastique de l'offre. En d'autres termes, l'utilisateur peut – pratiquement à tout moment – augmenter sa demande de service. À titre d'exemple, il pourra augmenter la capacité de mémoire initialement de 100 giga pour la porter à 200 et ainsi de suite. Pour le peu qu'il ne tienne pas sous contrôle ces demandes d'augmentation, le montant à payer au CCP deviendra exorbitant et peut-être fatal à son équilibre financier.

– L'« éclatement » des données d'une même personne dans divers endroits d'hébergement sans que l'utilisateur n'en soit réellement informé et donc en dehors de tout contrôle de sa part. Ces serveurs peuvent être situés dans des pays qui ne garantissent pas une confidentialité de niveau européen compte tenu des lois de police qui y sont d'application. Nous pouvons très aisément relever que certains pays connaissant un régime policier n'offrent pas une protection adéquate et qu'il y ait un risque certain (avéré ?) de violation de la confidentialité par les autorités nationales.

Il faut donc attirer l'attention des utilisateurs – tant privés que professionnels – sur ces aspects non exhaustifs qui peuvent atténuer l'engouement pour le *cloud computing*.

6. NIST a également défini quatre types de *cloud computing*, à savoir :

– *Cloud privé :* le fournisseur n'opère le *cloud computing* que pour une seule organisation, dans ses locaux ou pas, et qui l'administre seul ou avec un tiers. On peut se demander si nous nous trouvons réellement en présence d'un système de *cloud computing*, surtout s'il est dans les locaux de l'utilisateur. Nous aurions tendance

à sortir ce type-ci de la notion de *cloud computing* et d'autant plus lorsqu'il est dans cette dernière hypothèse.

- *Cloud communautaire :* l'infrastructure *cloud computing* est partagée par plusieurs personnes qui mettent en commun des services/préoccupations telles que la sécurité, des polices vie privée, etc. Cette infrastructure peut être sur site ou hors site. Nous sommes en droit de nous poser la même question que celle au sujet du *cloud* privé bien que l'on se rapproche de la notion de *cloud computing*.
- *Cloud public :* le fournisseur offre des services de *cloud computing* accessibles par le public en général, toutes personnes confondues (physiques et morales).
- *Cloud mixte :* il s'agit d'un mélange de plusieurs types de *cloud computing* avec les réserves émises ci-dessus.

7. Trois modèles de services sont également identifiés par le NIST, à savoir :

- *Software as a service (SaaS) :* le fournisseur met à disposition des utilisateurs des logiciels qui ne sont pas modifiables ou personnalisables d'un point de vue fonctionnalité. Dans ce modèle, l'utilisateur peut seulement profiter du service tel qu'il est proposé.
- *Platforme as a service (PaaS) :* le fournisseur met à disposition une plate-forme fonctionnelle sur laquelle l'utilisateur pourra installer ses propres services/logiciels.
- *Infrastruture as a service (IaaS) :* le fournisseur fournit une infrastructure « vide » (*hardware*) qui pourra être utilisée par l'utilisateur pour y installer un OS et ses applications.

Au-delà de ces aspects purement matériels, attardons-nous à ceux concernant la protection des données à caractère personnel qui circulent dans le *cloud computing*.

Si trois modèles de services sont identifiés, chacun présente des questions identiques au niveau de la protection des données à caractère personnel dont l'identification des responsables de traitement et sous-traitants, l'identification des utilisateurs voulant accéder à leurs services, etc.

Dans la présente contribution, nous analyserons les concepts de responsable de traitement, de sous-traitant, d'information et de sécurité/confidentialité. Nous aborderons également un secteur qui ne pourrait faire appel au *cloud computing* pour les raisons que nous évoquerons et mettre en lumière certains points spécifiques.

Par contre, nous n'aborderons pas la question relative au fait que ni la directive 95/46/CE ni la loi Vie privée n'offre de protection aux personnes morales dès lors que seules les personnes physiques sont qualifiées de personnes concernées[6].

II. RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT[7]

8. La loi Vie privée en Belgique et la directive 95/46/CE au niveau européen, ont mis en place divers acteurs dont le responsable de traitement et son sous-traitant.

6 Voy. à ce propos Y. Poullet, J.-M. Van Gyseghem, J. Gérard, C. Gayrel et J.-P. Moiny, « Cloud computing and its implications on data protection », *Discussions Paper for the Council of Europe's project on Cloud Computing*, Namur, mars 2010, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

7 Voy. également ENISA, « Cloud Computing, Benefits, Risks and Recommendations for Information Security », novembre 2009, www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

Il est utile, dans le cadre du *cloud computing*, de les identifier et de les replacer dans leur contexte, objet de la présente contribution.

Le Groupe de travail de l'article 29 (groupe de l'article 29) a émis un avis[8] dans lequel il définit de manière plus ample ces deux notions sans, malheureusement, toujours y apporter la clarté espérée. Ainsi que nous le verrons, l'avis donne l'impression de s'être écarté de l'esprit de la directive pour assurer une protection supérieure. Cette manière de procéder ne peut cependant être suivie car il faut, à certaines occasions, montrer l'incomplétude de certaines règles pour inviter les autorités à les amender afin qu'elles soient adaptées à la réalité du terrain. Une loi – ou directive – ne peut se permettre d'être « tordue » au risque de la décrédibiliser, de l'affaiblir.

9. La loi Vie privée définit le responsable de traitement comme étant la « personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, *détermine les finalités et les moyens* du traitement de données à caractère personnel »[9].

Le Groupe 29 a précisé cette définition en considérant que :

> « 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. C'est pourquoi un critère purement formel ne suffirait pas, pour au moins deux raisons : dans certains cas, la désignation officielle d'un responsable du traitement (prévue, par exemple, par la loi, dans un contrat ou dans une notification à l'autorité chargée de la protection des données) fera tout simplement défaut ; dans d'autres cas, il se peut que la désignation officielle ne reflète pas la réalité, les fonctions de responsable du traitement étant confiées à un organisme qui, dans les faits, n'est pas en mesure de "déterminer".
> L'affaire *Swift* démontre bien l'importance de l'influence de fait : la société Swift était officiellement considérée comme le sous-traitant des données alors qu'en réalité, elle intervenait, au moins dans une certaine mesure, en tant que responsable du traitement des données. Il a ainsi été clairement établi que, même si la désignation d'une entité en tant que responsable du traitement ou sous-traitant des données dans un contrat pouvait révéler des informations intéressantes sur le statut juridique de l'entité, cette désignation contractuelle ne permet cependant pas de déterminer avec certitude son véritable statut, qui doit être déduit de circonstances concrètes.
> Cette approche factuelle est du reste corroborée par le fait que, selon la directive, le responsable du traitement est celui qui "détermine" plutôt que celui qui "détermine licitement" les finalités et les moyens. C'est l'identification même de la responsabilité du traitement qui est primordiale, quand bien même la désignation se révèlerait irrégulière ou le traitement des données serait réalisé de manière illicite. Peu importe que la décision de traiter des données soit "licite", au sens où l'entité qui a pris la décision y était juridiquement habilitée ou qu'un responsable du traitement a été officiellement désigné selon la procédure requise. La question de la licéité du traitement des données à caractère personnel revêtira encore son importance à un stade ultérieur et sera examinée à la lumière d'autres articles (notamment les articles 6 à 8) de la directive. En d'autres termes, il importe de faire en sorte que, même en

[8] Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf.

[9] Article 1er, § 4, de la loi Vie privée ; nous soulignons.

cas de traitement illicite des données, un responsable du traitement puisse être facilement identifié et désigné comme tel »[10].

Cependant et pour permettre aux personnes concernées, par exemple, d'identifier le responsable de traitement, le Groupe 29 a déterminé des catégories permettant « d'aborder ces questions de façon systématique »[11] :

- la responsabilité découlant d'une compétence explicitement donnée par la loi ;
- la responsabilité découlant d'une compétence implicite ;
- la responsabilité découlant d'une influence de fait.

Dans le cadre du *cloud computing*, il est rare que l'on se trouve dans une des premières catégories de sorte que l'on devra procéder à une réelle analyse factuelle pour déterminer le responsable de traitement.

Donc, seule la dernière nous intéresse dans le cadre du *cloud computing* qui est expliquée par le Groupe 29 comme suit :

> « Il s'agit du cas où la responsabilité du traitement est attribuée après une évaluation des circonstances factuelles. Un examen des relations contractuelles entre les différentes parties concernées sera bien souvent nécessaire. Cette évaluation permet de tirer des conclusions externes, attribuant le rôle et les obligations de responsable du traitement à une ou plusieurs parties. Elle peut s'avérer particulièrement utile dans des environnements complexes, exploitant les nouvelles technologies de l'information, dans lesquels les acteurs concernés ont fréquemment tendance à se considérer comme des "médiateurs" et non comme des responsables du traitement consciencieux.

Il peut arriver qu'un contrat ne désigne aucun responsable du traitement mais qu'il contienne suffisamment d'éléments pour attribuer cette responsabilité à une personne qui exerce apparemment un rôle prédominant à cet égard. Il se peut également que le contrat soit plus explicite en ce qui concerne le responsable du traitement. S'il n'y a aucune raison de penser que les clauses contractuelles ne reflètent pas exactement la réalité, rien ne s'oppose à leur application. Les clauses d'un contrat ne sont toutefois pas toujours déterminantes, car les parties auraient alors la possibilité d'attribuer la responsabilité à qui elles l'entendent.

Le fait même qu'une personne détermine comment les données à caractère personnel sont traitées peut entraîner la qualification de responsable du traitement, même si cette qualification sort du cadre d'une relation contractuelle ou si elle est expressément exclue par un contrat. L'affaire *Swift* en est un exemple éloquent : cette société a pris la décision de mettre à disposition certaines données à caractère personnel (lesquelles étaient initialement traitées à des fins commerciales pour le compte d'établissements financiers) également pour lutter contre le financement du terrorisme, comme le demandaient les injonctions adressées par le Trésor américain.

En cas de doute, d'autres éléments que les clauses d'un contrat peuvent servir à identifier le responsable du traitement, tels

[10] Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 8.

[11] Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 10.

> que le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables que cette visibilité peut susciter chez ces dernières (voy. également les explications ci-dessous concernant le troisième élément du point b)). Cette catégorie est particulièrement importante puisqu'elle permet d'examiner les responsabilités et de les attribuer également en cas de comportement illicite consistant à traiter des données contre les intérêts et la volonté de certaines des parties »[12].

Si, de prime abord, il semble aisé de déterminer le responsable de traitement, cela l'est moins dans la réalité. Certaines situations pratiques rendent extrêmement difficile la détermination de la personne qui, réellement, détermine les finalités et les moyens du traitement. Pensons au domaine médical dans lequel le patient pourrait très bien être considéré comme la personne qui procède à cette détermination. Mais il en va de même pour le professionnel de la santé. Qui est qui ? Sont-ils coresponsables ?

10. Par ailleurs, le sous-traitant est défini, dans la loi Vie privée, 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 »[13].

Le Groupe 29 a, à nouveau, précisé cette notion en estimant que :

> « L'existence d'un sous-traitant dépend du responsable du traitement, qui peut décider soit de traiter les données au sein de son organisation, par exemple en habilitant des collaborateurs à traiter les données sous son autorité directe (voir, *a contrario*, l'article 2, point f)), soit de déléguer tout ou partie des activités de traitement à une organisation extérieure, comme l'indique l'exposé des motifs de la proposition modifiée de la Commission, par "une personne juridiquement distincte du responsable mais agissant pour son compte".
>
> Par conséquent, les deux conditions fondamentales pour agir en qualité de sous-traitant sont, d'une part, d'être une entité juridique distincte du responsable du traitement et, d'autre part, de traiter les données à caractère personnel pour le compte de ce dernier. L'activité de traitement peut se limiter à une tâche ou un contexte bien précis, ou être plus générale et étendue.
>
> En outre, le rôle de sous-traitant ne découle pas de la nature de l'entité traitant des données mais de ses activités concrètes dans un cadre précis. En d'autres termes, la même entité peut agir à la fois en qualité de responsable du traitement pour certaines opérations de traitement et en tant que sous-traitant pour d'autres opérations, et la qualification de responsable ou de sous-traitant doit être évaluée au regard d'un ensemble spécifique de données ou d'opérations »[14].

11. Dans le cadre du *cloud computing*, il faut nécessairement analyser le concept même du système.

Le CCP met à disposition de l'utilisateur des services qui varient en termes d'achèvement (cela va du *hardware* jusqu'au logiciel de cour-

[12] Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 12.

[13] Article 1er, § 5, de la loi Vie privée.

[14] Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, pp. 26-27.

riel ou bureautique). Il s'agit donc d'une offre de services.

À côté ou conjointement à ces services, le CCP offre des garanties de sécurité et il en fait, à certains moments, un argument commercial tel Google avec son gmail.

La question essentielle est de déterminer qui est qui et qui détermine quoi.

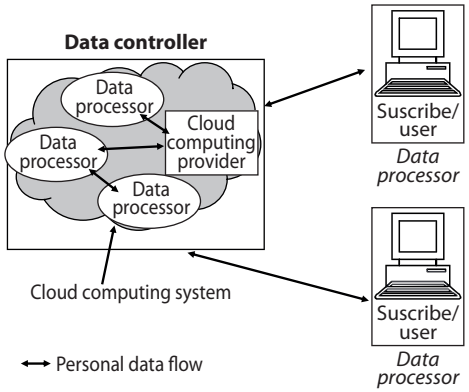
Diverses situations, qui se soutiennent l'une l'autre, s'ouvrent à notre analyse :

– Le CCP est le responsable de traitement car il déterminerait les finalités et les moyens de traitement. Le Groupe 29 a estimé devoir classer les réseaux sociaux, que nous classerons dans le *cloud computing*, dans cette catégorie dans les termes suivants :

> « Les fournisseurs de réseaux sociaux proposent des plateformes de communication en ligne qui permettent aux utilisateurs de publier et d'échanger des informations avec d'autres utilisateurs. Ces fournisseurs de services sont des responsables du traitement car ils déterminent à la fois les finalités et les moyens du traitement de ces informations. Les utilisateurs de ces réseaux, qui chargent également les données à caractère personnel de tiers, pourraient être responsables du traitement à condition que leurs activités ne soient pas soumises à "l'exemption domestique" »[15].

L'avis 5/2009 n'est guère plus explicite sur la décision du Groupe 29 de considérer les réseaux sociaux – qui doivent être considérés comme offrant des services de *cloud computing* –, comme étant exclusivement responsables de traitement.

Cela donnerait le schéma suivant[16] :



L'on doit cependant analyser les réseaux sociaux et constater qu'ils mettent à disposition d'utilisateurs une plateforme d'échange. Ces derniers s'y connectent et y chargent un certain nombre d'informations leur permettant d'entrer en relation avec d'autres internautes.

En analysant le comportement des utilisateurs et en ayant la définition de responsable de traitement à l'esprit, on peut considérer qu'ils déterminent eux-mêmes la finalité du traitement qu'ils effectuent tout autant que les moyens mis en œuvre pour l'atteindre.

En termes de finalité, on peut très logiquement considérer que les utilisateurs veulent, par la mise en œuvre du traitement, établir des relations avec d'autres utilisateurs du service. Pour y parvenir, ils déterminent un moyen efficace qui est l'utilisation du service offert par le réseau social choisi. Il nous paraît dès lors logique de considérer que les utilisateurs sont responsables de traitement sous réserve

15 Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 25 ; voy. également Groupe 29, avis 5/2009 sur les réseaux sociaux, 12 juin 2009, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_fr.pdf ; la notion de *cloud computing* peut être remplacée par celle de *social network* pour coller à l'avis du groupe 29.

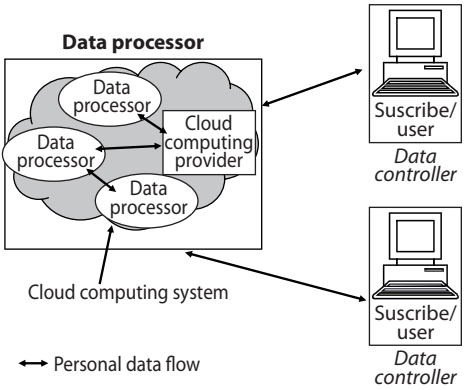
16 Y. Poullet, J.-M. Van Gyseghem, J. Gérard, C. Gayrel et J.-P. Moiny, « Cloud computing and its implications on data protection », *Discussions Paper for the Council of Europe's project on Cloud Computing*, Namur, mars 2010, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

de l'exclusion du champ d'application de la loi Vie privée prévue à son article 3, § 2, tel qu'analysé ci-dessus.

Cette analyse nous semble encore plus logique lorsque l'on parle de *cloud computing* comme offrant un accès à des services de bureautique par exemple ou de mise à disposition d'une plateforme ou encore d'une infrastructure. Il apparaît, en effet, assez clair que le CCP n'offre qu'un service qui sera utilisé par l'utilisateur à sa meilleure convenance ; utilisateur qui y traitera les informations dans le respect des principes légaux et sous son entière responsabilité.

Il y logera, par exemple, son programme de comptabilité avec les données comptables qui, souvent contiendra également des données à caractère personnel. Ce programme génère des factures concernant des personnes physiques protégées par la loi Vie privée. Il pourra également y loger ou utiliser un traitement de texte qui consistera en une partie du traitement au sens de la loi Vie privée. Il peut également s'agir de documents relatifs aux travailleurs tels que les fiches individuelles, etc. Immanquablement, l'utilisateur (société commerciale ou indépendant), d'une façon ou d'une autre, a un traitement de données à caractère personnel.

Nous constatons donc que l'application de la définition de « responsable de traitement » aboutit à une solution diamétralement opposée à celle prônée par le Groupe 29 et peut être représentée comme suit[17] :



Il est fort probable que la réflexion du Groupe 29 ait abouti à la solution critiquée compte tenu du peu de capacité du « faible » responsable de traitement, en la personne de l'utilisateur. La solution proposée par le Groupe 29 permettait ainsi de mieux contrôler les CCP, en leur qualité de responsable de traitement. Mais un tel contrôle, assez illusoire au demeurant, autorise-t-il de manipuler la directive 95/46 et, partant, la loi Vie privée ainsi que les définitions qu'elles contiennent ? Nous ne le pensons pas. Par contre, il serait utile de relever les inadéquations de certaines règles afin que les législateurs européens et nationaux les adaptent à la réalité des nouvelles technologies en perpétuelle mutation.

L'analyse que nous proposons n'empêche cependant pas de pouvoir considérer le réseau social/CCP comme responsable de traitement pour le traitement de données à caractère personnel effectué pour des finalités qui lui sont propres telles qu'une offre publicitaire personnalisée par le biais d'un *profiling* des utilisateurs. Il ne s'agit plus ici d'une offre de service offerte à l'utilisateur comme analysée ci-dessus mais bien d'un service ajouté pour lequel le réseau social/CCP détermine la finalité et les moyens mis en œuvre.

Une telle situation est parfaitement envisageable et probablement déjà envisagée par les acteurs sur le marché. Certaines sociétés

[17] Y. Poullet, J.-M. Van Gyseghem, J. Gérard, C. Gayrel et J.-P. Moiny, « Cloud computing and its implications on data protection », *Discussions Paper for the Council of Europe's project on Cloud Computing*, Namur, mars 2010, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

commerciales optent pour le *cloud computing* et y placent donc leurs données, en ce compris la comptabilité. Il serait aisé pour un CCP de proposer à ces sociétés de traiter les données comptables pour offrir certains services à valeur ajoutée tel que le classement des employés en fonction de leur déclaration de frais de représentation mensuelle.

Nous pourrions également imaginer un CCP qui procèderait à des croisements de données pour offrir à certains clients le profil financier des autres.

Nous constatons donc que les services à valeur ajoutée sont légion et peuvent être offerts par les CCP en leur qualité de responsable de traitement.

– Le CCP est sous-traitant. Ainsi que nous l'avons vu ci-dessus, il nous semble plus cohérent de considérer l'utilisateur comme responsable de traitement tandis que le CCP en serait le sous-traitant.

Cela signifie qu'en vertu tant de la loi Vie privée que de la directive 95/46, le sous-traitant, le CCP, ne pourra agir que sur instruction du responsable de traitement, l'utilisateur.

Se pose alors la question de connaître exactement le degré de contrainte que peut avoir l'utilisateur, bien souvent des P.M.E. ou des indépendants, face à des géants de l'Internet. Peut-il réellement imposer ses règles d'autant plus que, bien souvent, le CCP est établi hors du territoire européen ?

Dans son avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », le Groupe 29 avait donné un exemple de sous-traitance d'une plateforme de courriel et du problème de relation entre sous-traitant et responsable de traitement et le traitait comme suit :

> « John Smith recherche une plateforme de courriel qu'il pourrait utiliser avec les cinq employés de sa société. Il découvre qu'une plateforme conviviale conforme à ses besoins (également la seule proposée gratuitement) conserve les données à caractère personnel pendant une durée excessive et qu'elle les transfère à des pays tiers sans aucune garantie appropriée. En outre, les clauses contractuelles sont "à prendre ou à laisser".
>
> Dans cet exemple, M. Smith devrait soit chercher un autre fournisseur soit, en cas de non-respect allégué des règles de protection des données ou d'absence sur le marché d'autres fournisseurs adaptés, en référer aux autorités compétentes, par exemple celles chargées de la protection des données, les associations de protection des consommateurs et les autorités de la concurrence, etc. »[18].

Le problème posé par le Groupe 29 est applicable au *cloud computing* qui offre un marché de fournisseurs extrêmement pauvre à l'heure actuelle. Cependant, la solution donnée par ce même Groupe 29 est cependant peu applicable à moins d'instaurer le système de *class action* et/ou des autorités de contrôle réellement indépendantes et capables de procéder au contrôle nécessaire pour permettre à l'utilisateur de « négocier » avec les CCP. Cela semble cependant un vœu pieu et irréaliste face au marché actuel.

– Le CCP et l'utilisateur sont coresponsables du traitement. Au regard de ce qui a été relevé lors de l'analyse des deux premiers points, cette troisième situation paraît peu envisageable.

[18] Groupe 29, avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf, p. 28.

III. OBLIGATIONS DES RESPONSABLES DE TRAITEMENT ET SOUS-TRAITANTS

12. Après avoir déterminé les fonctions, il nous appartient d'analyser la question des obligations du responsable du traitement en en isolant deux.

Il est certain que le responsable de traitement, à savoir l'utilisateur de services, est tenu – en vertu de la loi Vie privée – à un certain nombre d'obligations. Dans le cadre de la présente contribution, nous en analyserons certaines qui nous paraissent intéressantes.

A. Obligation d'information

13. Le responsable de traitement doit délivrer une information aux personnes concernées[19] qui pourraient être les clients, les fournisseurs ou même les employés.

Cette obligation d'information découle, purement et simplement, de l'application du principe de transparence ainsi que l'a rappelé la Professeure de Terwangne en 2005 à l'occasion du colloque organisé par l'O.B.F.G. sur « cabinets d'avocats et technologies de l'information : balises et enjeux »[20]. Jean Herveg estime, à juste titre, que l'information s'inscrit également dans le principe de loyauté[21] et a rappelé qu'elle « participe à la "volonté d'assurer à l'individu une transparence des circuits informationnels (…)" »[22].

La question est de déterminer l'ampleur de cette information. Le responsable de traitement doit-il informer la personne concernée de l'utilisation du *cloud computing* dans le cadre du traitement mis en œuvre ? Partant du fait que l'obligation d'information est une application des principes de transparence et de loyauté, il nous paraît important que la personne concernée soit informée du fait que le responsable de traitement recoure au *cloud computing* afin de lui permettre de prendre sa décision en toute connaissance de cause si le traitement est fondé sur le consentement et d'exercer un contrôle accru sur les traitements dans l'hypothèse où le traitement ait une autre base de légitimation que le consentement.

En effet, le *cloud computing* pouvant entraîner un risque en matière de protection des données à caractère personnel, il semble important que la personne concernée en soit dûment informée afin qu'elle puisse exercer les droits qui lui sont accordés par la loi Vie privée.

B. Obligation de sécurité et de confidentialité

14. Le responsable de traitement sera également tenu à une obligation de sécurité et de confidentialité[23]. Cela implique qu'il devra prendre des mesures adéquates tant au niveau organisationnel que technique.

Cela touche, bien entendu, le choix du sous-traitant. Ainsi, il devra s'assurer que son choix se porte sur « un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements »[24].

En matière de sécurité, le responsable de traitement fait régulièrement appel à un sous-traitant spécialisé. Il en va de même dans le *cloud computing* puisque le CCP, sous-traitant ainsi que cela a été analysé ci-dessus, mettra en œuvre des garanties de sécurité des données qui circulent dans le *cloud*.

19 Article 9 de la loi Vie privée.

20 C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », in *Cabinets d'avocats et technologies de l'information : balises et enjeux*, Bruxelles, Bruylant, 2005, p. 169.

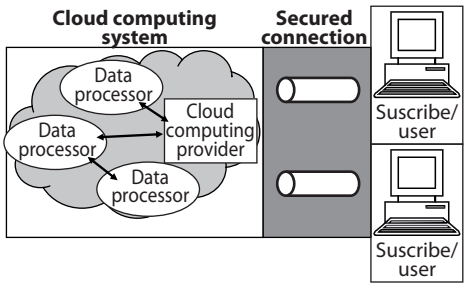
21 J. Herveg, *La protection des données du patient dans l'hôpital*, Kluwer, 2009, p. 48.

22 J. Herveg, *La protection des données du patient dans l'hôpital*, Kluwer, 2009, p. 48.

23 Article 16 de la loi Vie privée.

24 Article 16, 1°, de la loi Vie privée.

La situation peut être représentée comme suit[25]:



Ainsi que cela est représenté sur ce schéma, la sécurité devra être garantie à divers niveaux:

– le premier est la connexion elle-même entre l'utilisateur, responsable de traitement, et le *cloud computing*. Il faudra mettre des mesures techniques garantissant cette sécurité sans pour autant ralentir de manière trop sévère le flux; ralentissement qui pourrait être néfaste au service proposé.
– Le second est le *cloud* lui-même qui devra avoir un niveau de sécurité suffisant et répondant aux règles de l'art.

Dans l'absolu, les diverses mesures adoptées dans le respect des règles de l'art devraient permettre également de garantir la confidentialité exigée par l'article 16 de la loi Vie privée.

Cette obligation de confidentialité pourrait, dans le cadre du *cloud computing*, se trouver malmenée si les données sont hébergées – à l'initiative du CCP et dans le cadre de la maximalisation de ses services – dans des pays de type dictatorial ou totalitaire. Le CCP peut-il garantir la confidentialité alors que des lois de police sont susceptibles de permettre aux autorités d'accéder aux données? Cette incapacité ne rejaillit-elle pas sur le responsable de traitement qui n'a pas fait choix d'un sous-traitant apportant «des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements»[26].

À la lecture de l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant» du Groupe 29, il nous paraît que la réponse doit être positive. Pourrait-il alors faire valoir l'exonération de responsabilité prévue à l'article 15*bis*, alinéa 3, de la loi Vie privée? La question appelle une réponse très prudente. On pourrait, en effet, estimer que le dommage que subirait la personne concernée serait imputable au responsable de traitement dès lors qu'il ne s'est pas assuré de la qualité de son sous-traitant et surtout que les données ne seraient pas hébergées dans des serveurs localisés dans des pays ne garantissant pas un niveau de protection adéquat. Cela repose la question de la capacité du responsable de traitement d'imposer des règles d'hébergement au CCP et de la nécessité éventuelle de prévoir des contraintes légales garantissant un niveau de protection adéquat. Cela est d'autant plus difficile pour lui qu'il est contraint de signer des contrats d'adhésion ne lui permettant aucune marge de manœuvre.

Il découle de tout cela que la position de l'utilisateur est très inconfortable face à des paramètres qu'il est incapable de maîtriser car hors de sa capacité de négociation.

À l'heure actuelle et tant que le responsable de traitement sera soumis à des contrats d'adhésion, le responsable de traitement devra bien réfléchir aux risques pris s'il opte pour la solution du *cloud computing*.

Par ailleurs, ces contrats d'adhésion pourraient ne pas répondre aux conditions imposées par

[25] Y. Poullet, J.-M. Van Gyseghem, J. Gérard, C. Gayrel et J.-P. Moiny, «Cloud computing and its implications on data protection», *Discussions Paper for the Council of Europe's project on Cloud Computing*, Namur, mars 2010, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

[26] Article 16, 1°, de la loi Vie privée.

l'article 16 de la loi Vie privée. En effet, il est imposé au responsable de traitement de :

> « 1° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements ;
> 2° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles ;
> 3° fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement ;
> 4° convenir avec le sous-traitant que celui-ci 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 ;
> 5° consigner par écrit ou sur un support électronique les éléments du contrat visés aux 3° et 4° relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 3 »[27].

Outre le premier point qui a déjà été analysé ci-dessus, on imagine très difficilement – car cela est impraticable en matière de contrat d'adhésion – que le responsable de traitement réussisse à fixer la responsabilité du CCP à son égard, qu'il convienne que le CCP et les personnes travaillant pour lui n'agissent que sur ses instructions et doivent respecter les prescriptions relatives à la protection des données à caractère personnel. Cela pourrait être d'autant plus difficile que le CCP se trouverait soumis à un régime légal différent de celui du responsable de traitement (pensons à des régimes autoritaires ou liberticides).

Par ailleurs, il faut également avoir égard à la problématique du transfert de données vers un pays non membre de l'Union européenne et donc hors du régime de la directive 95/46 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. En vertu des articles 21 et suivants de la loi Vie privée, le transfert ne peut, en règle générale, s'effectuer que si le pays tiers « assure un niveau de protection adéquat »[28] et dans le respect des dispositions de la loi Vie privée et de ses arrêtés d'exécution. Ce caractère adéquat du niveau de protection « s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données ; il est notamment tenu compte de la nature des données, de la finalité et de la durée du ou des traitements envisagés, des pays d'origine et de destination finale, des règles de droit, générales et sectorielles, en vigueur dans le pays en cause, ainsi que des règles professionnelles et des mesures de sécurité qui y sont respectées »[29] [30]. Le Roi peut également déterminer les « catégories de traitements de données à caractère personnel et dans quelles circonstances la transmission de données à caractère personnel vers des pays non membres de la Communauté européenne n'est pas autorisée »[31].

L'article 22 de la loi Vie privée prévoit cependant des dérogations à ces principes qui tiennent en, par exemple, le consentement indubitable de la personne concernée qui serait, dans le cas de l'utilisation du *cloud computing* par une P.M.E., toute personne dont

27 Article 16 de la loi Vie privée.

28 Article 21, § 1er, alinéa 1er, de la loi Vie privée.

29 Article 21, § 1er, alinéa 2, de la loi Vie privée.

30 La Commission européenne établit une liste de pays dont le niveau de protection est considéré comme adéquat (http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm). À noter également que la Commission européenne a prévu des clauses contractuelles standards pour les sous-traitants établis dans un pays tiers (hors Union européenne) : http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm.

31 Article 21, § 2, de la loi Vie privée.

on traite les données personnelles. Ce pourra être le travailleur si le département RH utilise le *cloud computing*, les clients, etc. On remarque d'emblée que le consentement indubitable s'avèrera difficile à obtenir.

D'autres situations peuvent servir de fondement au transfert de données vers un pays tiers mais qui, à chaque fois, font intervenir la notion de nécessité qu'il faut toujours analyser afin de déterminer quelle est la voie la moins dommageable d'un point de vue protection de la vie privée. Partant de ce principe, peut-on réellement estimer que le *cloud computing* – en son état actuel et eu égard aux contrats d'adhésion – soit la voie la moins dommageable au niveau de la protection de la vie privée et des données à caractère personnel ? Nous ne le pensons pas pour les raisons évoquées ci-dessus.

Le responsable de traitement devra donc avoir égard à cette problématique qui est omniprésente dans le *cloud computing* dès lors que les CCP sont soit en dehors de l'Union européenne, soit effectuent des traitements hors Union européenne.

Indubitablement, le processus de révision de la directive 95/46 devra prendre en compte ces réalités afin de pouvoir les appréhender et donner une réponse adéquate.

IV. LE *CLOUD COMPUTING* ET LES DONNÉES RELATIVES À LA SANTÉ EN MILIEU HOSPITALIER

15. Il nous semblait intéressant de clore cette contribution par l'analyse de la situation des données relatives à la santé en milieu hospitalier.

16. Les hôpitaux sont confrontés, de manière récurrente, à un problème de stockage des données médicales et, principalement, les images IRM ou Rx. Ils sont ainsi tentés de vouloir externaliser les données afin de répondre au besoin de place. Le *cloud computing* leur offre une opportunité intéressante par l'élasticité de son offre. Cela est-il possible pour les hôpitaux belges ?

Nous devons rappeler que l'arrêté royal du 10 juillet 2008 portant coordination de la loi relative aux hôpitaux et à d'autres établissements de soins précise, en son article 20, § 1er, que :

> « L'activité médicale doit faire l'objet d'une évaluation qualitative aussi bien interne qu'externe ; à cet effet, il faut, entre autres, tenir à jour pour chaque patient un dossier médical ; ce dossier est conservé à l'hôpital »[32].

Par ailleurs, les données relatives à la santé font l'objet d'une protection accrue via le secret professionnel qui impose des mesures encore plus strictes en matière de protection des données.

Ces deux éléments mis ensemble – et même pris séparément au demeurant – semblent empêcher, de manière absolue et en l'état de la législation, les hôpitaux d'externaliser une partie ou l'entièreté du traitement et encore plus lorsqu'il s'agit du *cloud computing*.

Le gestionnaire d'un hôpital ne devra même pas se poser de question et devra trouver la solution à son manque de place en dehors de tout *cloud computing*.

V. À TITRE DE CONCLUSION

17. Au terme de cette analyse, nous pouvons relever un certain nombre d'éléments qui

[32] Article 10 de l'arrêté royal du 10 juillet 2008 portant coordination de la loi relative aux hôpitaux et à d'autres établissements de soins, http://staatsbladclip.zita.be/moniteur/lois/2008/11/07/loi-2008024327.html ; nous soulignons.

tendent à attirer l'attention de sociétés commerciales ou d'indépendants susceptibles de faire appel au *cloud computing* pour réduire, par exemple, leurs coûts en informatique.

Dans un premier temps, il nous a semblé nécessaire de rappeler les définitions de responsable de traitement et sous-traitant ; analyse qui nous a permis de considérer que la P.M.E. ou l'indépendant devaient être considérés comme responsables de traitement dès lors qu'ils déterminent les finalités et les moyens mis en œuvre.

Il découle de cela qu'ils sont soumis à diverses obligations dont celle, et pas des moindres, de confidentialité et de sécurité. Or, le contexte dans lequel se meut le *cloud computing* rend difficile une telle garantie.

Cette difficulté tient au fait que le *cloud computing* est littéralement dans le brouillard à divers niveaux :

- l'utilisateur n'est pas informé des lieux d'hébergement des données avec ce que cela pose comme problème de traçabilité ou de risque d'intrusion par des autorités policières étrangères ;
- l'utilisateur n'est pas informé des règles d'accès aux données ni les éventuels traitements ultérieurs ;
- l'utilisateur ne reçoit pas de notification d'éventuels *security breaches* à l'instar de ce qui est prévu dans la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques telle que modifiée par la directive 2009/136/CE ;
- les contrats sont des contrats d'adhésion sur lesquels l'utilisateur n'a aucun contrôle et qui comportent souvent une clause de modification unilatérale[33].

Il apparaît donc que, dans la situation actuelle, l'arsenal légal ou contractuel ne permet pas au responsable de traitement d'être assuré du maintien des règles de protection des données à caractère personnel. Il y a donc des risques importants qui doivent amener les sociétés commerciales/les indépendants à en prendre la juste mesure car il y va de leur responsabilité et de leur crédibilité.

[33] À propos des contrats, voy. D. Gomez, « Cloud computing survey finds issues with some contracts », www.tgdaily.com/networking-features/52707-cloud-computing-survey-finds-issues-with-some-contracts ; S. Bradshaw, C. Millard et I. Walden, *Contracts for Clouds : Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*. Queen Mary School of Law Legal Studies Research Paper No. 63/2010.