CLOUD COMPUTING: OPPORTUNITÉS ET RISQUES POUR LES AVOCATS

SÉBASTIEN FANTI
Avocat au Barreau valaisan, certifié OMPI, notaire, Sion

Mots clés: cloud computing, sécurité, protection des données, avocat, responsabilité, principe de précaution, conseils

Le présent article offre un aperçu de ce que recouvre l'appellation de Cloud computing et a pour objectif, après avoir identifié les principaux enjeux juridiques, de fournir un panel de conseils aux avocats.

I. Notions fondamentales

1. Définition et distinctions

A) Liminairement et contextuellement

Le Cloud computing est un modèle permettant l'accès aisé et à la demande à un ensemble de ressources de calculs configurables pouvant être rapidement provisionnées et mises à disposition avec un effort d'administration ou des interactions avec le fournisseur de services minimes[1]. Bien que l'anglicisme soit largement répandu, il existe différentes francisations dont: informatique en nuage, informatique dématérialisée ou encore infonuagique.

Cette définition est un excellent prisme de la complexité tant technique que juridique de cette matière qui évolue à un rythme effréné. Elle ne correspond pas à un concept juridique précis[2], ce qui engendre l'application de normes diverses et complémentaires.

Alors que le *Web* a permis de rendre accessibles en tout temps et au plus grand nombre toutes les informations, le Cloud computing augure, de surcroît, de la possibilité d'accéder à des capacités de traitement et de calcul qui permettront de reproduire, de partager, d'analyser et d'enrichir ces informations. Ces capacités auraient été hors de portée des petites ou moyennes entreprises pour des raisons financières principalement, si de tels services n'avaient pas vu le jour. Celles-ci peuvent donc bénéficier d'outils conviviaux et ergonomiques sans avoir à consentir des investissements importants notamment en termes d'infrastructure, de maintenance ou de développement de logiciels.

Un très grand nombre de services de Cloud computing sont déjà régulièrement utilisés, notamment par des avocats[3]. Citons, à titre exemplatif, des services de messagerie électronique (Hotmail, Gmail), des réseaux sociaux (Facebook, LinkedIn), des applications à télécharger sur son smartphone ou sa tablette (Evernote, Google Drive, IncaMail).

La Commission européenne a identifié le développement du Cloud computing comme un enjeu majeur de l'évolution du commerce électronique durant les prochaines années[4].

En Suisse, le Centre d'évaluation des choix technologiques TA-SWISS[5] (www.ta-swiss.ch) a conduit durant l'année 2011 un projet intitulé *«Cloud Computing – L'informatique en nuage».* L'étude conclut en mettant en exergue le fait que pour la Suisse aussi, le Cloud computing n'est pas une vague promesse d'avenir, mais une forme d'utilisation de l'informatique qui est déjà en voie de s'établir et de s'imposer toujours plus fortement. La Confédération a développé une stratégie en matière de Cloud computing des autorités suisses[6]. Elle a donc, à l'instar de nos voisins

1 La définition est inspirée de celle adoptée par le National Institute of Standards and Technology; pour d'autres définitions, cf. notamment ROLAND PORTMANN, Cloud computing: Chancen und Risiken, digma 2012, p. 186; ROLF OPPLIGER, Sicherheit im Cloud Computing, digma 2012, p. 28; ADRIAN RUFENER, Cloud Computing, Revue de l'avocat 4/2012, p. 198.

2 Même si l'aspect contractuel est un élément fondamental, cf. Feuille d'information TA-SWISS (http://www.ta-swiss.ch/fr/cloud-computing/): *«à l'exception des considérations relatives à la protection des données, les éventuels problèmes juridiques susceptibles de résulter de l'informatique en nuage peuvent tous être réglés par des contrats adéquats».*

3 WOLFANG STRAUB, «*Clic informatique»:* qu'apportent l'informatique et les nouvelles technologies dans les études d'avocats? (1ére partie), Revue de l'avocat 11–12/2012, p. 516 ss; SÉBASTIEN FANTI, iPhone, iPad, Androïd: un gain d'efficacité pour l'avocat?, Plädoyer 5/10 du 7 octobre 2010, p. 50.

4 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, *«Exploiter le potentiel de l'informatique en nuage en Europe»,* COM(20129 529 final, 27 septembre 2012, disponible à cette adresse: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:FR:PDF.

5 Les recommandations émanant de ce centre de compétence des Académies suisses des sciences servent d'aide à la prise de décision par le Parlement et le Conseil fédéral, en particulier sur des sujets technologiques controversés.

6 Laquelle peut être consultée à cette adresse: http://www.isb.admin.ch/themen/architektur/00183/01368/01372/index.html?lang=fr.

européens, pris conscience de la nécessité d'initier une démarche résolue visant à adopter un cadre technique, juridique et économique propice au développement de ces services informatiques.

B) Les différents types de services[7]

On distingue, traditionnellement, trois formules principales d'accès au Cloud computing[8]:

- IaaS (Infrastructure as a Service) où le fournisseur offre un accès à un environnement technique sur lequel le client peut installer son propre système d'exploitation et ses propres logiciels applicatifs;
- PaaS (Platform as a Service) où l'utilisateur accepte d'utiliser l'environnement de développement mis à disposition par le fournisseur en vue de créer ses propres logiciels;
- SaaS (Software as a Service) où le fournisseur met à disposition des logiciels applicatifs directement utilisables pour traiter et stocker des données.

Les enjeux juridiques diffèrent évidemment en fonction de la formule choisie, notamment en ce qui concerne la responsabilité du fournisseur de service.

2. Quelques enjeux juridiques du Cloud computing

A) Prolégomènes

La diversité et la complexité des enjeux propres au Cloud computing ne permettent pas une analyse exhaustive. La nature immatérielle[9] et internationale de tels services génère des questions de droit international privé, tant sur le plan de la compétence que du droit applicable[10]. En sus, les données hébergées peuvent faire l'objet, à tout le moins potentiellement, de demandes d'accès ou de consultation par des autorités publiques nationales dans le cadre de leurs pouvoirs d'enquête ou de contrôle[11].

Dans le cadre limité de cette contribution, seules les questions relatives à la protection des données et celles liées aux aspects contractuels seront abordées, à l'aune des intérêts spécifiques liés à la profession d'avocat.

B) Protection des données personnelles

Sur le plan international, la Commission européenne a publié le 25 janvier 2012 une proposition de règlement en vue de réformer certains aspects du cadre règlementaire applicable[12]. En cas d'adoption, en l'état, cette proposition devrait clarifier les règles en matière de droit applicable et faire en sorte qu'une entreprise établie dans plusieurs États membres soit assujettie au droit d'un seul État membre en matière de privacy.

Le Préposé fédéral à la protection des données et à la transparence a émis un document[13] dans lequel il expose les dangers liés au Cloud computing et formule différentes recommandations. Parmi les risques principaux, citons la perte de contrôle sur les données (impossibilité de localisation), le manque de séparation et d'isolation des données, le non-respect des dispositions légales, l'accès d'autorités étrangères aux données, la captivité de l'utilisateur par rapport au prestataire, la perte et l'usage abusif des données, ainsi que les pannes de systèmes et/ou l'indisponibilité des ressources.

Fondamentalement, le traitement de données personnelles découlant de l'utilisation des services de Cloud computing relève du traitement de données par un tiers au sens de l'article 10a LPD. La première condition est que le traitement par un tiers est autorisé pour autant que la loi ou une convention le prévoie[14]. En sus différentes conditions sont émises, dont il résulte des obligations positives ténorisées dans les conseils que voici.

Le Préposé recommande:

- de n'effectuer que des traitements que le mandant peut effectuer lui-même (art. 10a al. 1 let. a LPD);
- de vérifier qu'aucune obligation légale ou contractuelle de garder le secret ne proscrive un tel traitement (secret professionnel, bancaire, médical, etc.);
- de s'assurer *in concreto* que le tiers assure effectivement la sécurité des données (art. 10a al. 2 LPD); il ne suffit donc pas de se fier aux assurances du prestataire, mais des vérifications concrètes, régulières, et *in situ* doivent être opérées (cf. 7 LPD, 8 ss et 20 ss OLPD); le prestataire doit protéger les données contre les risques suivants: destruction accidentelle ou non autorisée; perte accidentelle; erreurs techniques; falsification, vol ou utilisation illicite; modification, copie, accès ou autre traitement non autorisés;
- de s'assurer en cas de communication de données à l'étranger[15] de l'existence d'un niveau de protection adéquat (cf. art. 6 LPD), la preuve de la pertinence et de l'efficience des précautions prises incombant à celui qui transfère les données à l'étranger;

---

7 Cf. également ADRIAN RUFENER, Cloud Computing, Revue de l'avocat 4/2012, p. 198.

8 Ce sont les «service models»; pour une présentation exhaustive des différents services: http://fr.wikipedia.org/wiki/Cloud_computing, ainsi que le document de l'Académie suisse des sciences du 6 novembre 2012 intitulé *«White paper, Cloud computing»,* p. 8 ss, disponible à cette adresse: http://www.satw.ch/organisation/tpf/tpf_ict/box_feeder/2012-11-06_2_SATW_White_Paper_Cloud_Computing_EN.pdf.

9 Cf. également l'avis publié par le groupe article 29 le 1er juillet 2012, lequel contient des conseils précieux notamment en matière contractuelle: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

10 Sur cette problématique en matière de droits d'auteur, cf. VINCENT SALVADÉ, Le droit d'auteur dans le nuage ou dans le brouillard, sic!, 2012, p. 7.

11 En vertu du Patriot Act notamment, mais pas uniquement.

12 Ce document peut être consulté à cette adresse: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF.

13 Disponible à cette adresse: http://www.edoeb.admin.ch/themen/00794/01124/01768/index.html?lang=fr.

14 S'agissant de la loi, le libellé pourrait être «pour autant que la loi ne le proscrive pas».

15 Ce qui, sauf exceptions rarissimes, est la règle. Des exceptions existent en cas d'absence de niveau de protection adéquat: cf. art. 6 al. 2 LPD. Citons au titre des correctifs possibles les Safe Harbor principles, l'adoption de contrats ou le consentement préalable et éclairé.

– de s'assurer de l'accès en tout temps aux données (art. 8 LPD) et du droit d'effacer ou de rectifier les données (art. 5 LPD); le fait d'ignorer où ces données sont traitées n'exonère pas l'utilisateur de ces services de ces obligations légales.

C) Aspects contractuels

Dans la pratique, les fournisseurs de services invitent les utilisateurs, tant privés que professionnels, à signer sans réserve des contrats qui contiennent la plupart du temps des clauses désavantageuses. Parmi les clauses standardisées figure régulièrement un article stipulant une absence totale de responsabilité du fournisseur en cas de perte ou de destruction de données. Les risques inhérents à ces clauses contractuelles sont désormais bien identifiés[16]. Une négociation et une rédaction appropriées et fermes sont donc essentielles[17]. Il n'est pas simple d'obtenir une modification de tels contrats, ce qui signifie que seule une action concertée du plus grand nombre permettra à l'évidence d'obtenir des aménagements contractuels (cf. § 3/C et 4).

3. Spécificités liées à la profession d'avocat

A) Les risques spécifiques liés à la profession d'avocat

Voici à titre exemplatif et sans prétention d'exhaustivité les écueils auxquels devront faire face les avocats qui opteront pour de tels services informatiques:

– absence potentielle de confidentialité des données;
– absence de niveau de protection adéquat pour ces données;
– droit applicable et for s'agissant de ces données;
– clauses contractuelles exclusives de responsabilité rédigées en faveur du prestataire technique;
– cession éventuelle de propriété intellectuelle;
– accès d'autorités étrangères aux données;
– etc[18].

En sus du respect des normes, des étapes techniques de planification du recours à de tels services doivent être respectées:

– évaluation du caractère sensible des données traitées (dossiers pénaux, expertises psychiatriques, documents d'identité, etc.);
– évaluation des mesures de sécurité selon les normes internationales ISO 27001:2005 (gestion de la sécurité) et ISO 9001 (gestion de la qualité);
– comparaison préalable entre cloud et infrastructure interne;
– évaluation de la récupérabilité des données en cas de défaillance majeure ou de litige contractuel (plan B);
– adoption et implémentation de systèmes de secours …

B) L'environnement international

Le Conseil des barreaux européens (CCBE; www.ccbe.org) a émis le 7 septembre 2012 des lignes directrices *«sur l'usage des services d'informatique en nuage par les avocats»*[19]. Ces lignes directrices sont extrêmement précises et donc précieuses pour tous les avocats désireux de bénéficier des avantages de ces nouveaux services informatiques, tout en limitant les risques dans une mesure acceptable du point de vue légal et déontologique.

Leur transposition est possible et relativement aisée, quelles que soient les normes nationales dès lors que les principes et les règles à respecter sont similaires.

C) Régime juridique et déontologique applicable

En matière de *protection des données,* le régime légal a été exposé précédemment (§ 2/B) et les avocats qui entendent utiliser ces services devront respecter les règles précises évoquées. En vertu de l'article 11a al. 5 let. a LPD, les avocats ne sont, d'ordinaire, pas soumis à une obligation de déclaration de leurs fichiers. Cette exception se justifie par l'obligation imposée aux avocats en vertu de la LLCA de tenir des dossiers corrects complets et cohérents. Le Cloud computing est un mode de gestion des dossiers exogène et de surcroît facultatif, de sorte qu'une déclaration de fichiers est légalement nécessaire. Il convient également de préciser à l'attention des mandataires professionnels que l'exception précitée ne s'applique pas à tous les fichiers. Si certains sont tenus en l'absence d'obligation légale (par exemple pour établir des profils de clients), une déclaration est nécessaire[20].

En matière de *règles professionnelles,* ce sont les règles ordinaires qui trouvent application, soit celles figurant dans la LLCA et dans le Code suisse de déontologie. L'avocat doit donc s'assurer lui-même du respect de son secret professionnel notamment (art. 13 LLCA et art. 15 CSD). S'il est dans l'incapacité de le faire en raison notamment d'un refus du prestataire de révéler certaines informations (emplacement du serveur, sécurisation des données, etc.), il devra renoncer à utiliser ces services.

Relativement à la problématique *contractuelle,* il n'existe pas de recommandations de la FSA. Il convient donc de se référer aux lignes directrices du CCBE fort utiles pour la préparation et la négociation du contrat. Parmi les éléments qui doivent retenir l'attention figurent:

– les mesures de sécurité mises en place et les engagements pris à cet égard;
– les obligations attendues du fournisseur non seulement en termes de sécurité et de confidentialité, mais également en termes de disponibilité du service, de mise à

16 S. BRADSHAW, C. MILARD ET I. WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, Queen Mary University of London, Legal Studies Research Paper 63/2010 disponible sur le site www.cloudlegal.ccls.qmul.ac.uk.

17 Cf. à cet égard: SYLVAIN MARCHAND, Clauses contractuelles, Du Bon usage de la liberté contractuelle, Bâle 2008.

18 Cf. pour le surplus les lignes directrices du CCBE dont il est question au § 3/B.

19 Ces lignes directrices sont disponibles à cette adresse: http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/07092012_FR_CCBE_gui2_1347539443.pdf.

20 Cette remarque fait suite au constat selon lequel seuls quelques rares avocats ont émis une déclaration, alors que l'utilisation de logiciels de suivi de la relation client s'est généralisée dans les études d'importance.

jour des applications, de rapidité d'exécution, ainsi que d'effacement et de destruction des données après l'expiration du contrat;
- l'identification de tous les acteurs: courtiers, sous-traitants, intégrateurs, avec l'aménagement d'une procédure transparente et de possibilités de recours directs;
- la récupération des données en cas de rupture contractuelle et l'interopérabilité , respectivement la portabilité des données et le caractère réversible du recours aux services de Cloud computing;
- la gestion de la période de transition en fin de contrat, de manière à assurer certaines prestations telles que la remise des fichiers et des bases de données dans des formats prédéfinis compatibles avec l'environnement de l'utilisateur ou du fournisseur qui reprend le contrat.

4. Conclusions prospectives

Il serait souhaitable que la Fédération suisse des avocats établisse des contrats types de Cloud computing à l'intention de ses membres, de manière à uniformiser leurs exigences fondées sur les normes applicables à ces services informatiques et sur les règles prudentielles. Les prestataires de service se verraient soumettre un cahier des charges homogène fondé sur une analyse fine des risques. L'adoption de tels contrats devrait s'accompagner de la possibilité pour les membres de souscrire une assurance liée à ces services informatiques, dont chacun sait qu'ils ne sont pas infaillibles (assurance RC, perte d'exploitation, etc.).