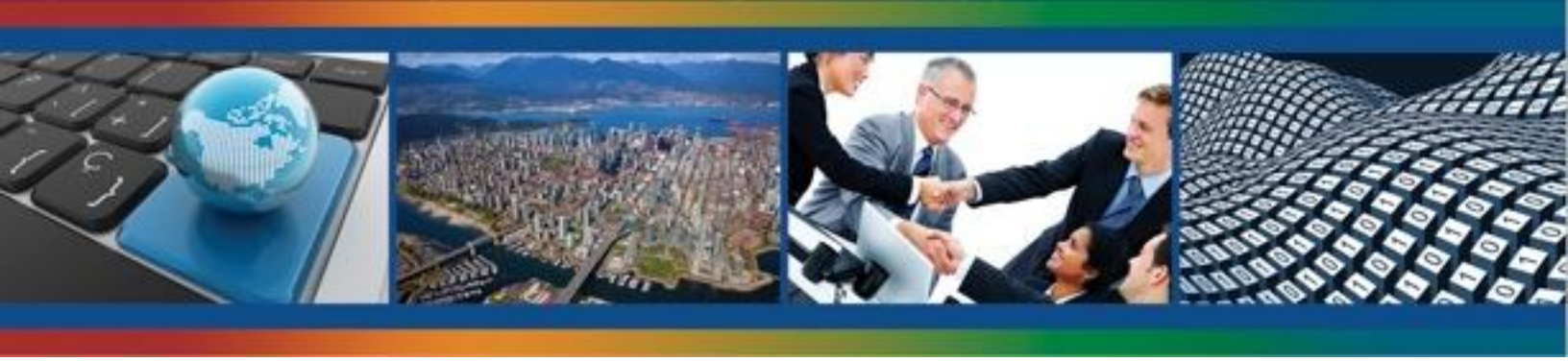


L'INFRASTRUCTURE CANADIENNE DE DONNÉES GÉOSPATIALES
PRODUIT D'INFORMATION 20f

Introduction : les conséquences stratégiques de l'information en nuage

Hickling Arthurs Low
Équipe de ressources chargée de la recherche et de l'analyse des politiques opérationnelles

2012

Ressources naturelles Canada | Natural Resources Canada

Canada

Table des matières

1. Préambule

Le présent guide fait partie d'une série de documents sur les politiques opérationnelles que GéoConnexions prépare actuellement. Il a pour but d'informer les intervenants de l'ICDG sur la nature et la portée de l'informatique en nuage et sur les réalités, les enjeux et les pratiques exemplaires en matière de politiques opérationnelles connexes.

L'informatique en nuage offre un accès souple, indépendamment du lieu, à des ressources informatiques qui sont rapidement et naturellement attribuées ou diffusées en réponse à la demande. Les nuages informatiques offrent de faire des calculs, fournissent des logiciels, offrent l'accès à des données et des ressources d'entreposage sans que les utilisateurs aient besoin de connaître les détails de l'infrastructure informatique. Pour les fournisseurs de données géospatiales et de logiciels, l'informatique en nuage représente un nouveau moyen potentiel de faire des affaires en offrant des options à faible coût ou gratuites aux clients afin qu'ils aient accès aux produits et services en ligne. Au lieu de se procurer un logiciel à mettre en œuvre à l'interne et de télécharger des bases de données complètes, les clients « louent » le logiciel et ont accès uniquement aux données dont ils ont besoin par le biais des services Web, et ce, lorsqu'ils en ont besoin. Le « nuage » devrait devenir le lieu de prédilection pour un large éventail d'utilisateurs amateurs de données géospatiales qui souhaitent accéder à cette puissante technologie et l'utiliser.

Le programme de **GéoConnexions** *est une initiative nationale dirigée par Ressources naturelles Canada. GéoConnexions appuie l'intégration et l'utilisation de l'***Infrastructure canadienne de données géospatiales (ICDG).**

*L'***ICDG** *est une ressource en ligne qui améliore le partage, l'accessibilité et l'utilisation de l'information géospatiale canadienne- l'information sur des lieux géographiques au Canada. Elle peut aider les décideurs de tous les ordres de gouvernement, du secteur privé, des organismes non gouvernementaux et du monde universitaire à prendre des décisions éclairées sur les priorités socioéconomiques et environnementales.*

Le passage à l'informatique en nuage semble inévitable. Le modèle des services partagés de technologie de l'information (SPTI) du gouvernement canadien prévoit une feuille de route sur l'informatique en nuage (Danek, 2010). Services partagés Canada est chargé de la prestation de certains services de TI pour le compte des ministères gouvernementaux, y compris la gestion du centre de données. À l'échelle provinciale, au moins deux gouvernements évaluent l'informatique en nuage. Le gouvernement de l'Ontario évalue le potentiel de l'informatique en nuage comme une meilleure façon d'utiliser et d'offrir des services en ligne (Microsoft, 2011). Dans son document stratégique sur la GI/TI, le gouvernement de la Colombie-Britannique cite le fait de tirer profit des services de l'informatique en nuage comme étant l'une des deux principales stratégies d'hébergement TI/GI pour la province (Bureau du dirigeant principal de l'information, 2011).

Sur la scène internationale, le gouvernement fédéral américain a proposé une politique intitulée « cloud-first » pour les nouvelles solutions informatiques gouvernementales (Zients, 2010). D'après les prévisions liées à l'adoption de l'informatique en nuage dans tous les secteurs par les États-Unis, l'augmentation des dépenses liées aux services dans le nuage se stabilisera à 14 milliards de dollars en 2014 par rapport à 3 milliards en février 2011. Selon un article du Financial Times paru en mai 2011, la

valeur du secteur de l'informatique en nuage à l'échelle mondiale pourrait atteindre 150 milliards de dollars d'ici 2014. D'autres prévisions sont différentes, mais toutes s'accordent sur le fait que l'informatique en nuage prend de l'ampleur. Le nombre croissant d'organisations déjà présentes dans le nuage illustre cette tendance.

Le guide présente les principales questions relatives aux politiques opérationnelles géospatiales, qui sont impératives pour la réussite de toute entreprise dans le domaine de l'informatique en nuage. Les politiques opérationnelles sont les lignes directrices, les directives et les politiques dont se sert une organisation pour gérer le cycle de vie des données géospatiales (c.-à-d. collecte, gestion, diffusion et utilisation).

Le présent guide pourra intéresser toute personne qui souhaite mieux connaître l'informatique en nuage et les éléments liés aux politiques opérationnelles, comme la responsabilité, la protection des renseignements personnels et la confidentialité, la sécurité, l'octroi de licence, le droit d'auteur, l'archivage, les règlements et les normes.

2. Introduction

2.1 Informatique en nuage

Le National Institute of Standards and Technology des États-Unis (NIST), reconnu comme un des principaux experts en informatique en nuage, définit l'informatique en nuage comme « un modèle qui permet d'offrir un accès au réseau généralisé, pratique et sur demande à un ensemble partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, entreposage, applications et services) qui peuvent rapidement être fournies et diffusées en requérant un effort de gestion minime ou peu d'interaction du fournisseur de service » (Mel et Grance, 2011). La Figure 1 illustre les composantes de l'informatique en nuage d'un point de vue fonctionnel. Les utilisateurs finaux peuvent accéder aux Application spécialisées du nuage (p. ex. logiciel du SIG) par le biais d'un navigateur Web ou d'une légère application mobile ou bureautique alors que les données et les logiciels commerciaux plus généraux sont entreposés sur des serveurs qui font partie de l'infrastructure dans un lieu distant. Les concepteurs d'applications de l'organisation utilisatrice peuvent se servir des services de langues de programmation et d'outils de la plateforme pour créer leurs propres applications. En plus de l'entreposage de données, l'infrastructure offre des éléments informatiques ou de traitement et de réseau.

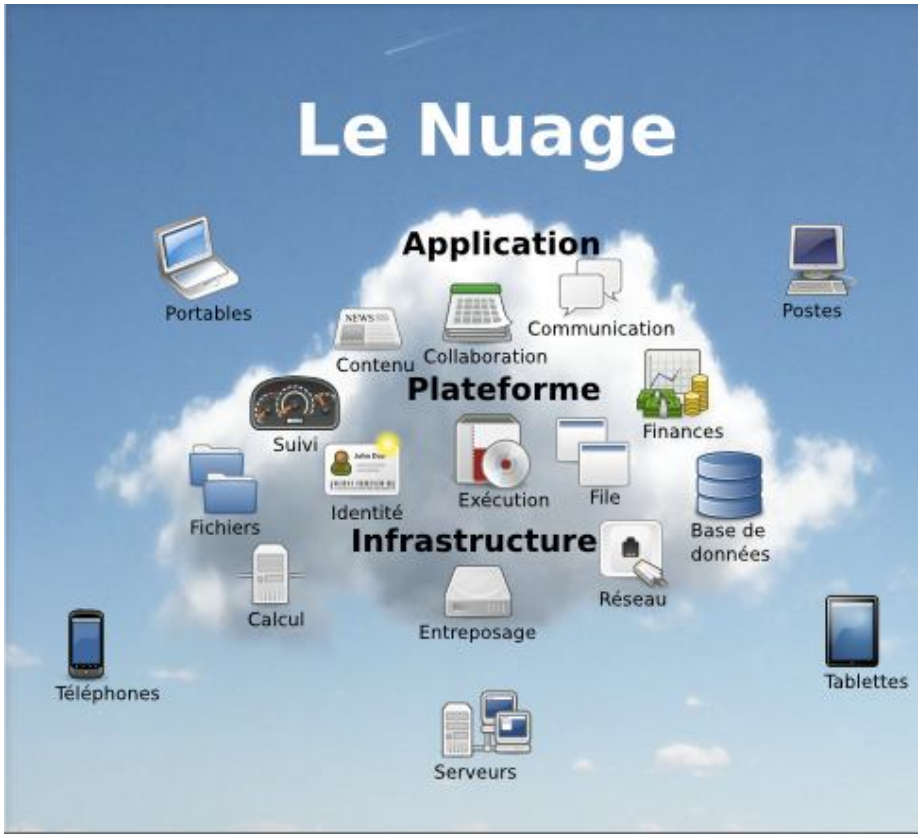


Figure 1 : Modèle fonctionnel de l'informatique en nuage
Source : Wikimedia Commons

2.2 Catégories de service de l'informatique en nuage

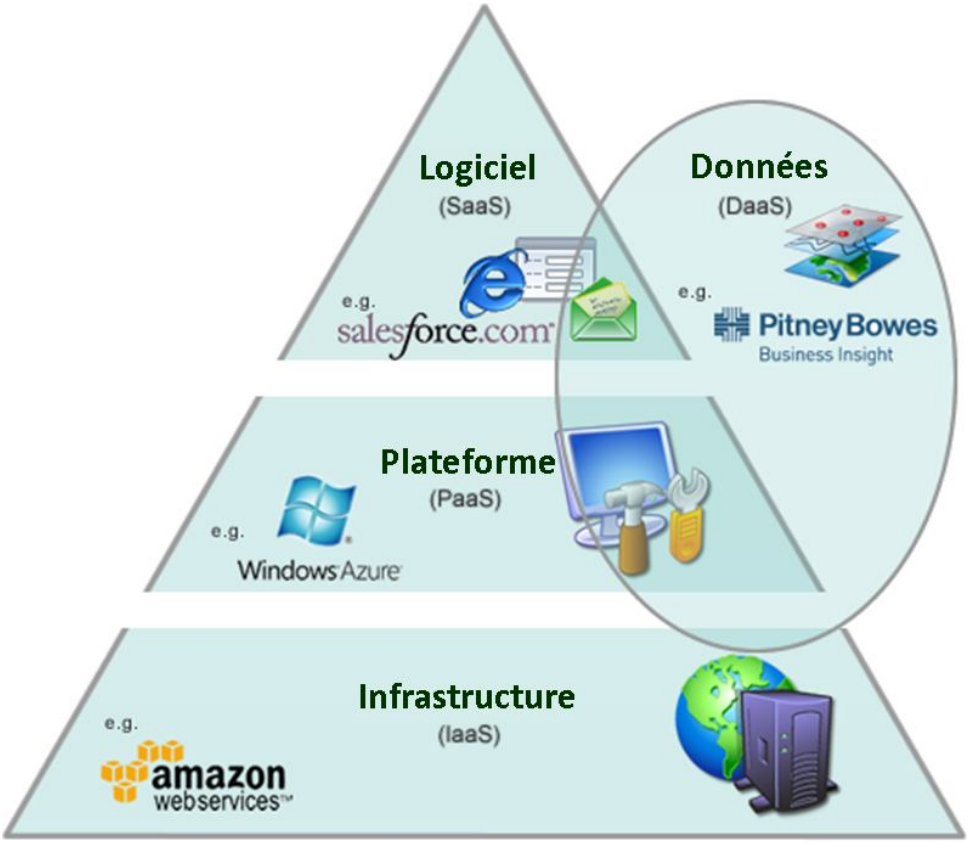
Aujourd'hui, l'informatique en nuage se manifeste dans l'une des quatre différentes catégories de service suivantes : infrastructure, plateforme, logiciel et données.

- *Infrastructure-service (IaaS)* : offre des ressources informatiques comme le traitement, l'entreposage et les réseaux. Les clients choisissent les ressources informatiques dont ils ont besoin. À gré de l'évolution de leurs besoins, on adapte le service du nuage. Les clients partagent la même infrastructure (entreposage, traitement, mémoire, réseau et machines virtuelles) et, en règle générale, l'emplacement physique de la ressource importe peu au client. Amazon Elastic Compute Cloud (EC2) en est un exemple connu.
- *Plateforme-service (PaaS)* : fournit aux organisations un environnement pour créer et déployer des applications en utilisant des langues et des outils de programmation pris en charge par le fournisseur, ainsi que l'infrastructure requise pour leur création. Azure Engine de Microsoft et App Engine de Google en sont de bons exemples.
- *Logiciel-service (SaaS)* : donne aux clients l'accès aux applications commerciales en ligne livrées avec l'infrastructure requise pour les supporter. La Salesforce.com, ArcGIS and the nuage d'Esri et la mise en œuvre du nuage en sont des exemples.
- *Données-service (DaaS)* : en règle générale mis en œuvre dans le cadre d'une solution SaaS, PaaS ou IaaS et fournit des données (souvent spatiales) dans les applications qui appuient la découverte de

données, l'accès aux données, leur manipulation et leur utilisation. Pour l'informatique en nuage géospatiale, les composantes des DaaS sont généralement essentielles, étant donné que la plupart des clients ont besoin de données spatiales de base comme Google Maps et/ou des cartes plus précises des frontières et thématiques pour leurs applications commerciales. Citons par exemple Pitney Bowes Data Insight's Data Market.

Les quatre catégories de service susmentionnées se recoupent ou se chevauchent et dans bien des cas, le service réel obtenu comportera des éléments de plusieurs catégories comme l'indique la Figure 2. Par exemple, l'Ontario Geoportal (géoportail de l'Ontario) fournit à diverses unités opérationnelles ministérielles des IaaS, SaaS et DaaS, mais pas de PaaS. En d'autres termes, l'Ontario GeoPortal fournit l'infrastructure technologique pour les systèmes opérationnels, un ensemble d'outils logiciels normalisés pour l'accès aux données et leur intégration ainsi qu'un grand nombre de données spatiales et de services d'une variété de sources. Toutefois, il ne s'agit pas d'une « plateforme » fournissant des outils et des widgets pour la création de nouvelles applications dans le nuage.

Figure 2 : Modèles de service de l'informatique en nuage



La Figure 3 illustre le grand éventail de fournisseurs de services d'informatique en nuage présents dans le marché aujourd'hui. Ces entreprises représentent une coupe transversale des utilisateurs des IaaS, PaaS, SaaS et DaaS dans les services d'informatique en nuage. Elles englobent certaines des meilleures entreprises du secteur des technologies de l'information ainsi que des entreprises du secteur de l'information géospatiale qui ont transféré leur logiciel et leurs données vers le nuage.

Figure 3 : Exemples de fournisseurs de services d'informatique en nuage

2.3 Options de déploiement de l'informatique en nuage

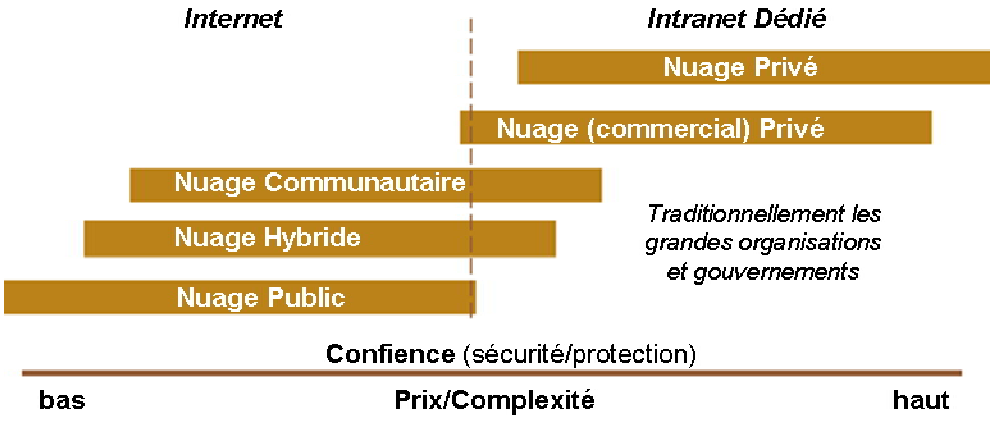
Les solutions dans le nuage sont déployées par le biais d'une des quatre méthodes suivantes : le nuage public, le nuage privé, le nuage communautaire ou le nuage hybride.

- *Nuage privé :* L'infrastructure en nuage est exploitée uniquement pour une organisation, dans ses locaux ou à l'extérieur et peut être gérée par l'organisation ou par un tiers.
- *Nuage communautaire :* Plusieurs organisations qui ont des points communs (p. ex. mission, exigences en matière de sécurité, politiques et questions de conformité) se partagent l'infrastructure en nuage, dans leurs locaux ou à l'extérieur. L'infrastructure et peut être gérée par les organisations ou par un tiers.
- *Nuage public :* L'infrastructure en nuage est rendue accessible au grand public ou à un grand groupe industriel et elle appartient à une organisation qui vend les services du nuage.
- *Nuage hybride :* L'infrastructure en nuage est composée d'au moins deux nuages (privé, communautaire ou public) qui sont liés par une technologie normalisée ou exclusive qui permet la portabilité des données et des applications.

La plupart des fournisseurs de services en nuage offrent leurs services dans un nuage public, étant donné que les options de nuage privé sont beaucoup plus coûteuses, car elles requièrent une infrastructure isolée et dédiée. Par conséquent, en règle générale, seules les grandes organisations, comme les ministères gouvernementaux, utilisent des nuages privés.

La Figure 4 illustre les types de déploiement de l'informatique en nuage et le niveau de « confiance » qui leur est associé, du point de vue de la protection des renseignements personnels et de la sécurité, ainsi que le coût relatif et les niveaux de complexité, dans les deux cas, dans un ordre croissant. Les solutions de la colonne de gauche sont offertes dans Internet, celles de la colonne de droite témoignent d'une utilisation accrue de l'intranet privé ou dédié.

Figure 4 : Options de déploiement de l'informatique en nuage



Certaines solutions dans le nuage, comme l'Ontario GeoPortal, proposent une « architecture répartie » qui permet l'intégration de la solution générale dans le nuage des données des clients qui sont trop

sensibles ou qui pour d'autres raisons ne peuvent pas être mises en œuvre dans le nuage en dehors du pare-feu de l'organisation.

En d'autres termes, il existe divers modèles et options de déploiement qui permettent de satisfaire aux besoins techniques d'une organisation et qui correspondent à sa tolérance en matière de sécurité.

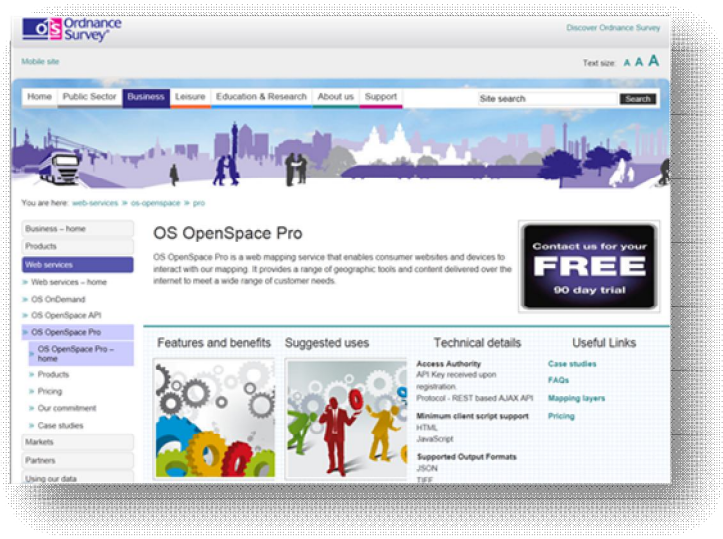
2.4 Informatique en nuage géospatiale

L'informatique en nuage géospatiale (ING) est un terme général employé pour décrire l'utilisation de l'informatique en nuage dans le domaine de l'information géospatiale. Il s'agit d'un service dans le nuage qui comporte des cartes et englobe l'utilisation et la manipulation de données spatiales. Une différence type entre l'ING et l'informatique en nuage est l'incorporation de données spatiales.

L'ING aide à populariser et à favoriser l'utilisation de cartes et de données géospatiales dans les systèmes opérationnels, comme le montre l'exemple sur Google Earth et l'Ontario GeoPortal présenté à la section suivante. Les solutions dans le nuage ouvrent la porte à un public élargi et à une mise en œuvre plus rapide et moins coûteuse que la mise en œuvre d'un SIG d'entreprise « classique » (Ontario GeoPortal, 2011). L'annexe 4 comporte une comparaison détaillée des solutions du nuage géospatial et du SIG d'entreprise (p. ex. applications et outils, infrastructure informatique, contenu, sécurité, coûts, etc.)

2.5 Utilisation de l'informatique en nuage

On a réalisé deux études de cas, une portant sur l'Ordnance Survey en Grande-Bretagne et l'autre sur l'Ontario GeoPortal, dans le cadre des recherches pour concevoir les présentes. On présente ici les leçons tirées de ces deux études de cas :



L'Ordnance Survey de la G.-B. est l'agence de cartographie nationale de la Grande-Bretagne. Depuis avril 2010, l'Ordnance Survey a rendu publique gratuitement une série de données afin de favoriser l'innovation et d'appuyer la transparence du gouvernement. L'Ordnance Survey utilise beaucoup l'informatique en nuage dans le cadre de ses services de cartographie Web, qui alimentent directement les sites Webs de clients ou les systèmes d'entreprises en données cartographiques du l'Ordnance Survey. L'Ordnance Survey a choisi d'héberger ses services sur la plateforme publique Amazon Web Services (AWS). Il est actuellement le plus gros utilisateur d'AWS du secteur public au R.-U. Son expérience avec Amazon a conduit l'Ordnance Survey à également réévaluer la façon dont il gère ses centres de données internes. L'Ordnance Survey a

récemment lancé un projet de consolidation qui vise à utiliser le matériel de base et la virtualisation pour construire une infrastructure de nuage privé plus efficace dans son centre de données.

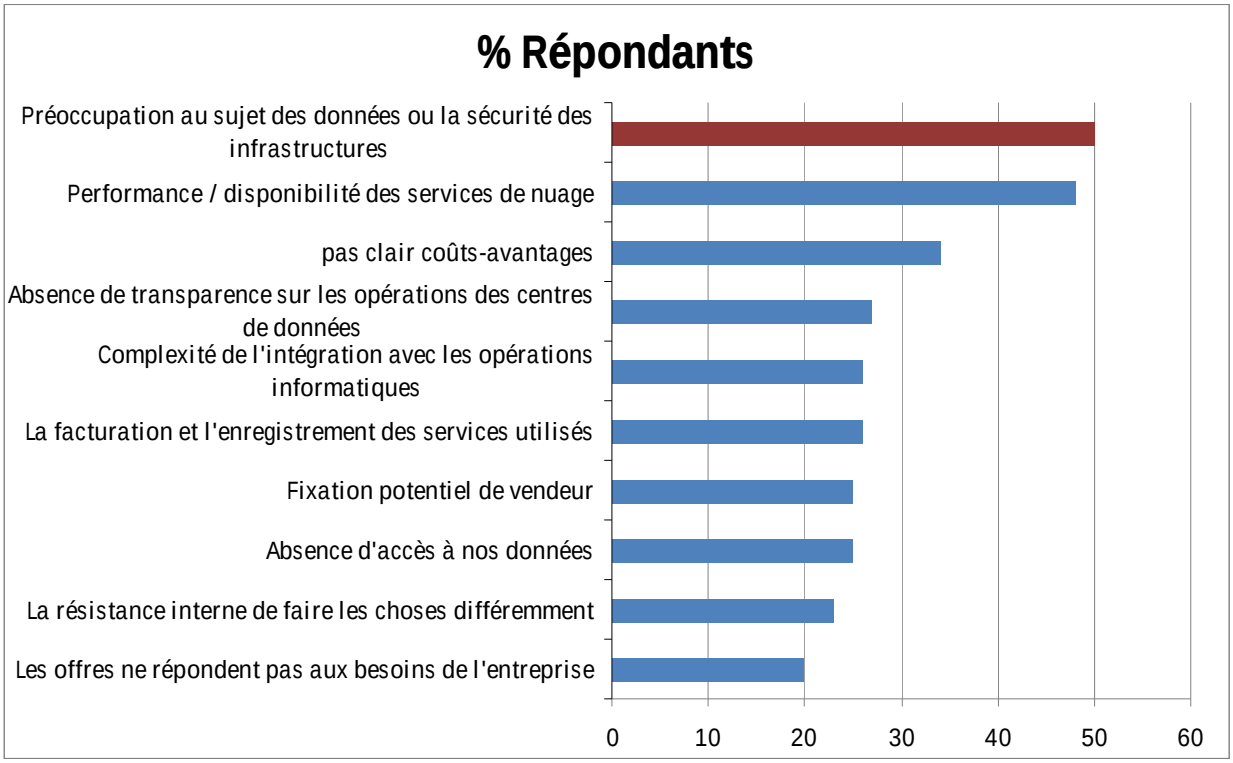
L'Ontario GeoPortal est un service hébergé de données, de logiciels et d'infrastructures d'Infrastructure Ontario, une société d'État chargée de gérer les biens immobiliers de la province : les biens, les terres et les édifices détenus ou loués. Alors que le service a été conçu au départ comme un SIG d'entreprise pour intégrer des données, des documents et des rapports provenant de diverses bases de données d'Ontario Realty Corporation (maintenant Infrastructure Ontario), ORC a décidé en 2009 de migrer les données, les logiciels et le matériel vers le « nuage » afin de continuer à faire évoluer le service en diminuant les besoins internes en TI et les coûts. À la base, l'Ontario GeoPortal sert de plateforme géographique pour intégrer, publier et visualiser les données opérationnelles tabulaires et le contenu non structuré et pour rendre ces renseignements accessibles aux utilisateurs, sans danger, par le biais d'une interface de cartographie. Le service compte actuellement plus de 1 600 utilisateurs au sein du gouvernement de l'Ontario et 14 applications ministérielles appuient une variété d'exigences opérationnelles.

3. Politiques opérationnelles et mise en œuvre de l'informatique en nuage

Les recherches menées pour préparer cette introduction indiquent clairement que la sécurité et la fiabilité des données, ainsi que le rendement du service dans le nuage sont les principales préoccupations des utilisateurs potentiels de l'informatique en nuage. Malgré l'expansion rapide de l'utilisation de l'informatique en nuage, certains problèmes freinent encore son adoption, comme l'indique la Figure 5 (Trend Micro, 2011) (Gens, 2009). Les fournisseurs de services parviennent difficilement à convaincre : a) que les données ne seront pas compromises; et b) que leurs services seront toujours accessibles et fiables.

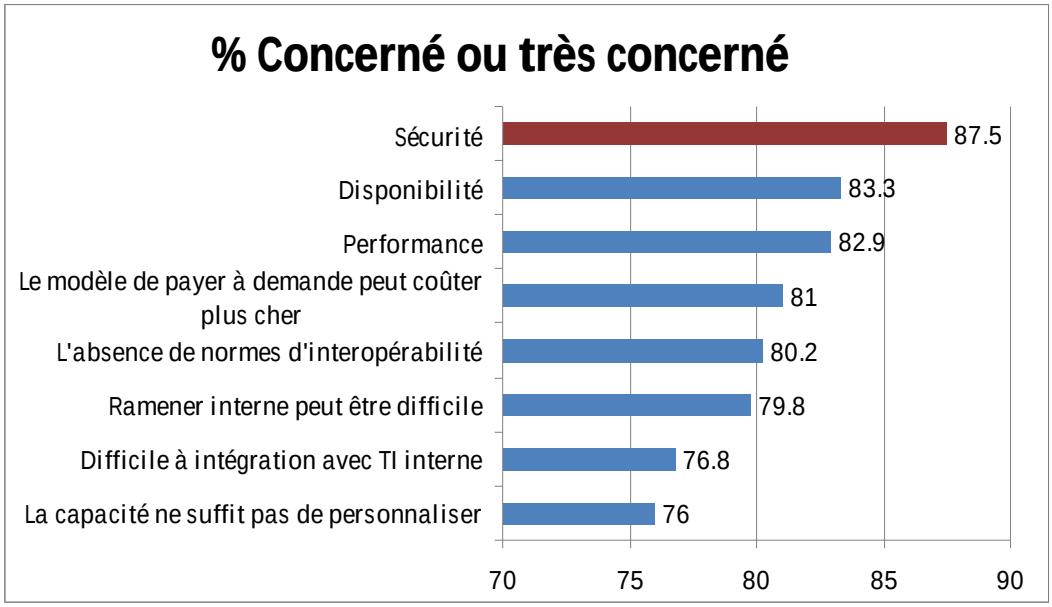
Figure 5 : Facteurs susceptibles d'inhiber l'adoption de l'informatique en nuage

Q. Quels risques ou obstacles percevez-vous quant à l'adoption de services d'informatique dans le nuage?



Source : Cloud Security Survey Global Executive Summary (Trend Micro, 2011)

Q. Notez les enjeux/problèmes du modèle du nuage/à la demande.



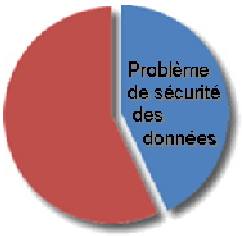
Source : New IDC IT Cloud Services Survey: Top Benefits and Challenges (Gens, 2009)

3.1 Sécurité

3.1.1 Risques liés à la sécurité dans le nuage

La sécurité est la principale préoccupation en ce qui a trait à l'informatique en nuage, tant pour ce qui est de l'accès non autorisé aux données que de la capacité du système à contrecarrer les attaques malveillantes. Voici quelques **risques liés à la sécurité** (Cloud Security Alliance, 2010) (Weech, 2011) :

- *Utilisation abusive et malveillante de l'informatique en nuage* – Les fournisseurs d'informatique en nuage sont la cible des polluposteurs, des auteurs de programmes malveillants et d'autres criminels.
- *Interfaces de programmation d'applications non sécurisées* – Les interfaces et les API de mauvaise qualité exposent les utilisateurs de l'informatique en nuage à des risques liés à la confidentialité, à l'intégrité, à l'accessibilité et à la responsabilité.
- *Personnes internes malveillantes* – L'utilisation abusive interne peut nuire à la marque et entraîner des pertes financières et de productivité.
- *Vulnérabilités de la technologie partagée* – Les menaces qui ciblent les activités d'une organisation peuvent avoir des répercussions sur beaucoup d'autres personnes qui partagent les mêmes ressources.
- *Perte/fuite de données*– L'utilisation inadéquate des données ou l'accès inadéquat aux données peut entraver la confiance, avoir des conséquences financières et sur l'aspect concurrentiel et entraîner des infractions et des conséquences juridiques.
- *Détournement des comptes, des services et des échanges*– Les contrevenants qui utilisent des comptes volés peuvent compromettre la confidentialité, l'intégrité et l'accessibilité des services d'informatique dans le nuage.
- *Profil de risque inconnu* – L'absence d'évaluation adéquate des risques et des menaces peut rendre les clients vulnérables.
- *Complexité* – La complexité de l'infrastructure en nuage, ainsi que l'intégration dans l'infrastructure interne de l'organisation, peuvent donner davantage d'occasions d'exploiter la sécurité.
- *Délégation de pouvoir* – La sécurité est confiée à votre fournisseur.
- *Chiffrement* – Devient encore plus difficile lorsque les clés sont conservées hors site.



Les préoccupations relatives à la sécurité semblent être bien fondées. D'après le sondage mené en mai 2011 par Trend Micro auprès de 1 200 décideurs, 43 % des répondants à l'échelle internationale (38 % au Canada) qui utilisaient un service d'informatique dans le nuage avaient signalé un problème ou une défaillance de la sécurité des données cette année-là. Toujours d'après le même sondage, 50 % des répondants ont indiqué que les problèmes de sécurité sont l'une des principales raisons pour ne pas adopter l'informatique en nuage, et 40 % de ceux qui utilisaient une solution d'informatique en nuage avaient l'impression que leurs besoins en matière de sécurité TI n'étaient pas satisfaits.

Entente clientèle
Amazon Web Services
« **Vous êtes tenu** de configurer et d'utiliser adéquatement les offres de services [AWS] et de prendre les mesures qu'il faut **pour assurer la sécurité, la protection et la sauvegarde de votre contenu**. Vous pouvez notamment utiliser des technologies de chiffrement pour protéger votre contenu de l'accès non autorisé et archiver régulièrement votre contenu. »

Toutefois, certains utilisateurs de l'informatique en nuage pensent que le nuage offre une possibilité *accrue* en matière de sécurité pour les raisons suivantes (Jackson, 2011) :

- Les systèmes font l'objet de correctifs de la sécurité en même temps;
- On a besoin de peu de personnes pour mettre les systèmes à jour;
- Les fournisseurs ont un fort désir d'assurer la sécurité de leur service.

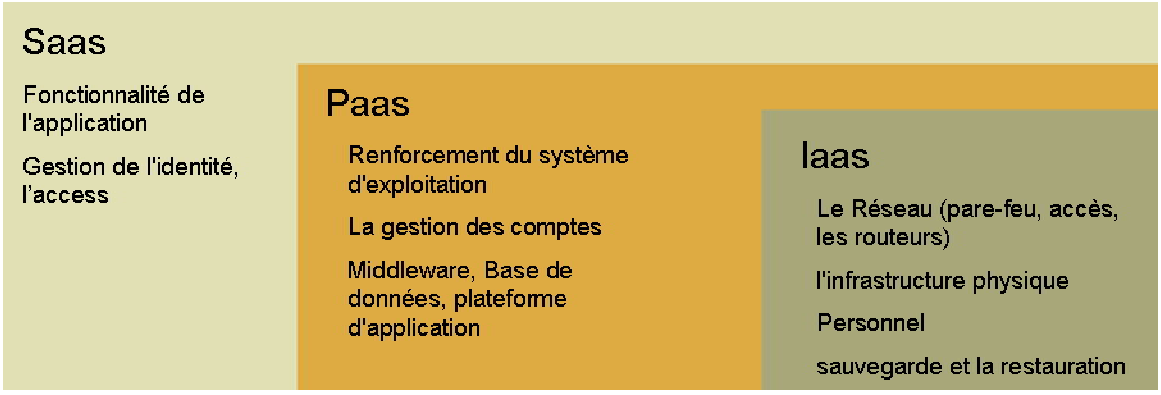
Les experts comme la Cloud Security Alliance et l'European Network and Information Security Agency ont publié de précieux conseils sur la gestion des risques liés à la sécurité dans un environnement d'informatique en nuage (Cloud Security Alliance, 2011) et (European Network and Information Security Agency, 2009a).

3.1.2 Responsabilité

Il est essentiel de comprendre le concept de **responsabilité** afin de gérer la sécurité des solutions dans le nuage. La Figure 6 illustre les types de mécanismes de contrôle de la sécurité de chaque modèle prédominant de service d'informatique dans le nuage. Normalement, les fournisseurs de services d'informatique en nuage sont responsables de la sécurité générale des systèmes alors que la sécurité des données et de l'accès au contenu (qui a accès à quoi et comment) incombe au client.

Les fournisseurs d'informatique en nuage sont en règle générale très discrets sur leurs capacités en matière de sécurité. Ils s'engagent en général à respecter un ensemble de normes et de processus pour atténuer les atteintes à la sécurité, mais ils ne garantissent *pas* qu'aucune atteinte n'aura lieu. Selon le type de services dans le nuage, les organisations peuvent être responsables de la sécurité des données placées dans le nuage, des applications qu'ils conçoivent et des systèmes d'exploitation qu'ils mettent au point.

Figure 6 : Mécanismes de sécurité par type de service



Source : Adapté de (Sawyer, 2011)

3.1.3 Évaluation des risques et des menaces

ÉVALUATION DES RISQUES ET DES MENACES

Avant le lancement de l'Ontario GeoPortal, on a mené une évaluation des risques de menaces (ERM) adéquate. On a embauché un cabinet d'experts-conseils spécialisé en sécurité des TI pour réaliser l'ERM. On a ensuite examiné les problèmes indiqués dans le rapport. Les nouveaux clients d'Ontario GeoPortal ont accès au rapport de l'ERM afin qu'ils puissent réaliser leur propre analyse des risques de menaces que représente la solution.

La réalisation d'une **évaluation des risques et des menaces** (ERM) est de façon générale perçue comme une pratique exemplaire. Toutefois, certains fournisseurs d'informatique en nuage peuvent ne pas autoriser le genre de vérification normalement réalisée pendant une ERM. L'ERM permet de déterminer les principaux éléments (c.-à-d. les composantes de l'infrastructure), services et données qui composent la solution d'informatique en nuage et les environnements connexes. Elle permet de déterminer la sensibilité de ces éléments et d'évaluer les menaces potentielles, les vulnérabilités et les méthodes de protection. Les risques sont souvent « cotés » comme étant faibles, modérés, élevés et graves. Dans le cadre de l'ERM, on fournit des recommandations pour aider à atténuer les risques pour atteindre les objectifs définis et améliorer la résilience et l'efficacité opérationnelles.

L'ERM tiendra compte des éléments suivants : l'accessibilité au service et son exploitation continue; la confidentialité et la sécurité des principales données; les liens avec d'autres services et systèmes externes; et la confiance et la collaboration des partenaires et des utilisateurs. Elle analyse ce qui suit :

- Le système général et ses livrables
- Les clients
- Les composantes du système
- L'architecture des applications
- L'architecture du réseau
- Le contrôle de l'accès des utilisateurs
- Les mécanismes de sécurité de l'installation d'hébergement et des installations des clients
- Les normes et les exigences en matière de TI en vigueur

En fonction de cette enquête, l'ERM inclura les éléments suivants :

1. *Évaluation de la sensibilité* – noter et évaluer chaque élément lié à la confidentialité, l'intégrité et l'accessibilité.
2. *Évaluation des menaces* – déterminer et décrire les menaces qui pèsent sur le système et les effets potentiels sur les attributs relatifs à la confidentialité, l'intégrité et l'accessibilité des données et des biens.
3. *Évaluation de la vulnérabilité* – examiner le système afin de repérer les faiblesses ou les défaillances en matière de protection.
4. *Évaluation du risque* – quantifier la mesure dans laquelle un risque donné est acceptable.

3.1.4 Atténuation des risques

Les organisations peuvent résoudre les problèmes de sécurité en utilisant une variété de pratiques exemplaires d'**atténuation des risques**. Par exemple (Drake, Jacob, Simpson, et Thompson, 2011) (Escalante et Korty, 2011) :

- Les utilisateurs qui décident que les risques d'atteinte à la sécurité sont d'une telle gravité qu'ils préfèrent ne pas déployer d'applications dans des nuages publics peuvent choisir à la place d'utiliser des nuages privés protégés par un pare-feu, dans leurs locaux, afin de gérer les problèmes liés à la protection des renseignements personnels, la sécurité et l'authentification.
- Une organisation peut utiliser des nuages publics, mais insister pour que ses données ne soient pas conservées sur des serveurs qui se trouvent dans des endroits faisant l'objet d'atteintes à la sécurité (p. ex. sur le territoire américain ou sous le contrôle d'une entreprise établie ou affiliée aux États-Unis, en raison des questions sur l'application de la Patriot Act).
- Les organisations peuvent profiter des coûts réduits des nuages publics tout en protégeant les renseignements sensibles, par exemple, en éliminant certains attributs des données géospatiales avant de les envoyer vers le nuage.
- Les organisations mettent en œuvre la sécurité partout (p. ex. transfert chiffré vers le nuage, codage sécurisé et contrôle de l'accès dans les applications et chiffrement des données stockées), à la place de la méthode normale de périmètre de sécurité.
- Les organisations peuvent s'assurer que l'ensemble des API et des sources de données est vérifié par le biais d'épreuves de pénétration[1] et qu'il est analysé en détail.
- Les organisations peuvent créer un énoncé de politique et des documents de formation sur les types de données autorisés sur les services d'informatique dans le nuage et établir un processus pour mener des examens de la sécurité, conformément à la politique.

[1] Méthode qui consiste à évaluer la sécurité d'un système ou d'un réseau informatique en simulant une attaque par une personne externe malveillante qui n'est pas autorisée à accéder aux systèmes de l'organisme et d'une personne interne malveillante qui dispose d'un certain niveau d'accès autorisé (Wikipédia, 2012)

3.1.5 Surveillance de la sécurité et réaction aux incidents

PERTINENCE DE LA SURVEILLANCE DE LA SÉCURITÉ ET DE LA RÉACTION AUX INCIDENTS DANS LE NUAGE

Les organismes doivent s'assurer que la surveillance de la sécurité et la réaction aux incidents sont convenablement prises en compte, en (Sawyer, 2011) :

- **Demandant aux fournisseurs d'IN le plus haut niveau d'accès et de contrôle ou des niveaux d'assurance prouvés acceptables par le biais du contrat et de l'ANS**
- **Demandant aux fournisseurs d'IN d'accéder à l'ensemble des registres sur la sécurité existants et les intégrer dans les processus internes de surveillance de la sécurité**
- **Élaborant et en appliquant un plan de réaction aux incidents adapté à leurs besoins et qui s'adapte au nuage**

Enfin, deux aspects portants sur la sécurité dans le nuage demeurent essentiels du point de vue de l'utilisateur : la **surveillance de la sécurité et la réaction aux incidents**. La capacité d'une organisation de surveiller ses données dans le nuage peut être limitée, car l'accessibilité aux registres de sécurité varie selon le modèle d'informatique en nuage et les fournisseurs de services dans le nuage peuvent également limiter les différents types de registres qu'ils rendent accessibles aux clients. La réaction aux incidents est plus compliquée dans le nuage, car il n'y a pas qu'un seul dispositif matériel à partir duquel on peut prélever et analyser des données. De plus, une coordination qui requiert beaucoup de temps s'avère également nécessaire pour régler un incident étant donné que les dispositifs touchés se trouvent dans les locaux du fournisseur de nuage et non dans ceux de l'organisation.

3.2 Protection des renseignements personnels et confidentialité

3.2.1 Risques liés à la protection des renseignements personnels et à la confidentialité dans le nuage

Les **risques liés à la protection des renseignements personnels et à la confidentialité** arrivent tout juste derrière les préoccupations liées à la sécurité qui découragent souvent les organisations à transférer leurs données et leurs applications vers le nuage. De plus, la protection des renseignements personnels ainsi que la confidentialité de certains types de données d'entreprises ou gouvernementales sont évidemment étroitement liées à la question de la sécurité des données. Ces préoccupations s'expliquent principalement par le fait que les fournisseurs de services d'informatique dans le nuage ont nécessairement accès aux données de l'utilisateur et qu'ils peuvent les divulguer ou les utiliser, accidentellement ou délibérément, à des fins non autorisées. Il faut protéger les données personnelles, confidentielles et sensibles, surtout contre l'accès inadéquat ou la perte. On peut résumer comme suit les principaux risques liés à la protection des renseignements personnels et la confidentialité en ce qui a trait à l'informatique en nuage (Gellman, 2009) (Commissariat à la protection de la vie privée du Canada, 2010) :

- *Conditions de service et politique sur la protection des renseignements personnels* – Les risques liés à la protection des renseignements personnels et la confidentialité peuvent varier grandement en fonction du fournisseur d'informatique en nuage.
- *Divulgation de renseignements à un fournisseur de nuage* – Pour certains types de renseignements et certaines catégories d'utilisateurs d'informatique en nuage, les droits, les obligations et le statut en matière de protection des renseignements personnels et de confidentialité peuvent changer en cas de divulgation.
- *Situation juridique et protections* – La divulgation et l'entreposage à distance peuvent avoir des effets néfastes sur les renseignements personnels et commerciaux.
- *Emplacement des renseignements dans le nuage* – Le lieu peut avoir d'importantes conséquences sur la protection des renseignements personnels et la confidentialité des données ainsi que sur les obligations en matière des personnes qui traitent et entreposent les données, ou les données peuvent être conservées à plusieurs emplacements à la fois, ce qui entraîne des conséquences juridiques différentes.
- *Obligations juridiques* – En vertu de la loi, un fournisseur de nuage peut être tenu d'examiner les données des utilisateurs afin de trouver des preuves d'activités criminelles ou pour d'autres motifs.
- *Incertitudes juridiques* – Il est difficile d'évaluer le statut des données dans le nuage, ainsi que les méthodes de protection des renseignements personnels et de confidentialité offertes aux utilisateurs.
- *Création de nouveaux flux de données* – Les fournisseurs d'informatique en nuage peuvent utiliser les données à des fins qui dépassent celles consenties au départ.
- *Intrusions dans les données des personnelles* – Les fournisseurs d'informatique en nuage ou d'applications dans le nuage peuvent accéder aux données qui sont en leur possession, les extraire ou les commercialiser sans que les propriétaires le sachent.

CONSÉQUENCES DE LA LPRPDE

Quelques effets de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) sur l'environnement de l'informatique en nuage au Canada (Karn, 2011) :

- **Les fournisseurs de nuage qui traitent des données personnelles doivent prévoir des méthodes de sécurité**
- **Les fournisseurs de nuage ne sont pas autorisés à conserver indéfiniment des renseignements personnels**
- **Les fournisseurs de nuage ne sont pas autorisés à utiliser des renseignements personnels ou leurs dérivés à de nouvelles fins**
- **Les utilisateurs de nuage doivent communiquer diverses autres obligations de la LPRPDE à leur fournisseur d'IN**

3.2.2 Questions relatives aux compétences

Les **questions relatives aux compétences** sont également une source importante de préoccupation en matière de protection des renseignements personnels. Par exemple, si des données du nuage sont conservées sur des serveurs qui se trouvent sur le sol américain, les fournisseurs de services pourraient communiquer les données des clients et leurs habitudes d'utilisation aux organisations gouvernementales s'ils n'ont pas obtenu d'autorisation adéquate (Weissberger, 2011c). La *Patriot Act* des États-Unis et la *Loi sur le Service canadien du renseignement de sécurité* du Canada comportent des dispositions qui obligent les fournisseurs d'informatique en nuage à remettre les données au gouvernement. De plus, si les données sont entreposées sur des serveurs qui se trouvent à plusieurs

endroits, la gestion du retrait du consentement relatif à l'utilisation des données devient beaucoup plus complexe.

Une des exigences liées à la création de l'Ontario GeoPortal était que le fournisseur de services retenu devait résider en Ontario et y entreposer les données, afin qu'il n'y ait pas de problèmes de compétences en ce qui a trait aux données hébergées. Dans le cas de l'Ordnance Survey, Amazon conserve ses données sur des serveurs à Dublin et le gouvernement britannique n'a pas tendance à entreposer des données personnelles à l'extérieur du R.-U. Bien qu'il pourrait techniquement demander une exemption, il a décidé qu'il serait plus facile de construire des solutions de façon à ne pas avoir besoin de conserver de données personnelles dans le nuage.

3.2.3 Obligations des fournisseurs dans le nuage

Comme il est indiqué plus haut, dans le contexte de la sécurité et selon le type de service fourni dans le nuage, le fournisseur de nuage peut avoir à jouer un rôle important en matière de confidentialité des données et de protection des renseignements personnels, ou il peut ne presque rien avoir à faire du tout. En règle générale, les fournisseurs de IaaS et PaaS jouent un rôle restreint pour assurer la protection des renseignements personnels et la confidentialité des données qu'ils conservent, sauf en ce qui a trait à l'accès des tiers ou à l'utilisation non autorisée des données qu'ils entreposent.

Au Canada, en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), les fournisseurs d'informatique en nuage qui traitent des renseignements personnels doivent se doter de méthodes de protection qui les empêchent de conserver des renseignements personnels indéfiniment ou de les utiliser à de nouvelles fins. Les organisations doivent savoir que, si leur fournisseur d'informatique en nuage se trouve à l'extérieur du Canada et qu'il utilise les données illégalement, il est probable que ce soient eux qui seront les plus touchées en cas d'enquête ou de sanctions.

Entente clientèle Salesforce.com
« Conformément à la *Master Subscription Agreement* [convention d'abonnement de base] de salesforce.com, **salesforce.com peut accéder aux données des clients uniquement afin d'offrir ses services, d'éviter ou de régler des problèmes de service ou techniques, à la demande des clients afin de les aider à résoudre un problème ou si la loi l'exige. »**

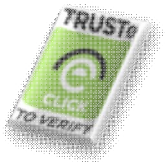
La plupart des pays ont des lois sur la protection des renseignements personnels, mais il semblerait que les politiques sur la protection des renseignements personnels des fournisseurs d'informatique en nuage n'en tiennent pas toujours compte (Ryan, 2011). En dépit de ces questions de protection des renseignements personnels, la réussite d'une entreprise comme Salesforce.com montre que bon nombre d'organisations consentent à confier leurs données les plus sensibles aux fournisseurs de services.

3.2.4 Atténuation des risques liés à la protection des renseignements personnels et à la confidentialité

Les organisations peuvent utiliser diverses méthodes pour atténuer les risques relatifs d'atteinte à la protection des renseignements personnels et à la confidentialité. Par exemple, les organisations qui

s'orientent vers l'informatique en nuage peuvent s'assurer que la personne chargée de la protection des renseignements personnels est présente dès le début du processus afin de veiller que les droits en matière de protection des renseignements personnels des particuliers soient déterminés et reconnus, et afin de repérer et traiter les risques potentiels liés à l'utilisation de l'informatique en nuage. Le personnel chargé de la protection des renseignements personnels doit participer à l'évaluation de l'information envoyée vers le nuage, du modèle de prestation de service proposé, de la proposition du fournisseur d'informatique en nuage avant d'octroyer un marché et d'autres secteurs d'intérêt liés à des lois données.

De plus, les organisations peuvent utiliser des technologies pour protéger les renseignements personnels, notamment le chiffrement des données avant de les téléverser vers le nuage, et des dispositifs de sécurité installés sur le matériel comme le Trusted Plateforme Module, conçu pour fournir à l'utilisateur à distance l'assurance que les données qu'ils envoient à un fournisseur d'informatique en nuage sont traitées conformément à la politique de l'entreprise uniquement. Les services comme TRUSTe offrent un service de vérification de la protection des renseignements personnels pour aider les fournisseurs d'informatique en nuage et les clients à gérer les problèmes de protection des renseignements personnels et de confidentialité. L'Annexe 3 donne d'autres conseils pour gérer les risques d'atteinte à la protection des renseignements personnels ou à la confidentialité dans le nuage.



3.3 Droit d'auteur et octroi de licences

Au Canada, il n'y a jusqu'à présent jamais eu d'affaire judiciaire traitant du **droit d'auteur** dans le contexte de l'informatique en nuage, mais plusieurs questions se posent dans les cercles juridiques, notamment sur les points suivants : quand et où des copies des travaux sont faites et par qui; les copies de secours et le transfert d'œuvres visées par des droits d'auteur d'un serveur à un autre dans le nuage; la propriété du fournisseur de services et de l'utilisateur ou l'octroi de licence des droits relatifs aux œuvres; l'existence du droit d'auteur dans le nuage ou le produit traité à partir du nuage; et le contrôle de la communication des travaux au-delà des frontières.

Le nuage a également donné lieu à des cas complexes d'**octroi de licence** pour les utilisateurs et les fournisseurs d'informatique en nuage. Par exemple, les modèles classiques d'octroi de licences de logiciels ne sont pas

OCTROI DE LICENCE DANS LE NUAGE

Infrastructure Ontario collabore avec divers fournisseurs de données afin de veiller à ce qu'un accès adéquat de ses données et une utilisation appropriée soient maintenus dans les différentes configurations des clients de l'Ontario GeoPortal. Par exemple, le ministère des Ressources naturelles a déjà négocié une entente afin de rendre accessible l'Ontario Parcel (OP), une base de données spatiales contenant les limites des propriétés de la province, à d'autres ministères, afin que l'Ontario GeoPortal puisse tirer profit de l'entente de l'OP. Le GeoPortal donne aux ministres qui autrement pourraient ne pas utiliser le grand et complexe OP un accès simplifié à la possibilité d'utiliser cette ressource.

Les fournisseurs de logiciels ont différentes méthodes d'octroi de licence pour les services d'IN et beaucoup parviennent difficilement à établir des tarifs adéquats. Pour l'Ordnance Survey (OS), le coût de l'utilisation de certains logiciels de sa solution d'IN était prohibitif, les logiciels Open Source ont donc été privilégiés. OS a fait très attention aux modèles de licence qui se cachent derrière certains logiciels afin de s'assurer de ne pas être obligé de rendre le logiciel, les données ou les services accessibles contre son gré.

compatibles avec le nuage et les nouveaux modèles évoluent, comme la facturation rétroactive en fonction des ressources ou du nombre d'utilisateurs desservis ou les frais mensuels à la demande en fonction des antécédents en termes de nombre d'utilisateurs ou de demandes enregistrées. Les fournisseurs de logiciels comme Microsoft, Oracle, Esri, etc. ont proposé des méthodes de tarification et d'accès conçues pour les fournisseurs d'informatique en nuage qui offrent des solutions IaaS, PaaS, voire même SaaS.

De plus, les fournisseurs de DaaS dans le nuage pourraient avoir des difficultés à gérer les licences multiples de fournisseurs de données tiers. Si les licences pour les différents ensembles de données qu'ils veulent offrir dans le cadre de leurs services sont assujetties à des conditions conflictuelles, ils doivent y remédier afin que les conditions du fournisseur de DaaS relatives à l'octroi de licence aux utilisateurs pour ses données soient utilisables. Par exemple, dans le cas de l'Ontario GeoPortal, il faut trouver le moyen de fournir différents niveaux d'accès aux données en raison des restrictions relatives à l'octroi de licence qui visent certains ensembles de données qui se trouvent sur le portail.

3.4 Questions juridiques/responsabilité

Il existe un éventail de questions juridiques liées à l'informatique en nuage. On en a déjà cité plusieurs dans les sections 3.2 et 3.3. Cependant, la plupart des questions ne sont pas propres au nuage et les clients potentiels de l'informatique en nuage pourraient se servir de l'analyse appliquée à d'autres services Internet comme fondement pour l'analyse des risques liés à la sécurité que représente l'informatique en nuage.

3.4.1 Contrats d'informatique en nuage

On constate un grand nombre de critiques dans la documentation au sujet des défauts des normes de services et des accords sur les niveaux de service (ANS) des fournisseurs d'informatique en nuage ainsi que sur le fait qu'ils soient en général peu enclins à modifier leurs **contrats** (Bradshaw, Millard, et Walden, 2010), (MacDonald, 2010), (Karn, 2011). Dans son cas, l'Ordnance Survey, a abordé l'engagement d'Amazon à fournir des services dans le nuage un peu comme l'impartition de tout autre élément de services ou d'infrastructure TI. Il a donc tenu compte de plusieurs points notamment, les méthodes de protection contre les modifications à environnement technique; les garanties et des indemnités relatives aux droits de propriété intellectuelle; les obligations en matière de sécurité, de copies de secours et de rétablissement après une catastrophe; et les dispositions relatives à la protection des données et à la confidentialité. Il n'a toutefois pas eu affaire au fameux manque de volonté de la part du fournisseur d'informatique en nuage à modifier ses conditions générales. L'OS a dû assumer toute responsabilité de tiers ou de ses utilisateurs finaux et accepter que les coûts ou les dommages découlant de toute omission dans la prestation de service dans le nuage ne puissent être récupérés auprès d'Amazon. Les ANS emploient souvent un langage vague et des définitions étroites sur les garanties de service, l'accès aux statistiques sur la qualité des services et le règlement de conflits, etc. L'OS a connu ce problème et a négocié une ANS personnalisée avec son fournisseur, Amazon.

En 2011, à l'occasion d'un atelier de Federated Press, intitulé Cloud Computing Law, on a présenté de précieux renseignements sur les questions juridiques relatives à l'informatique en nuage. Plus

particulièrement, deux conférences portaient sur les éventuels problèmes suivants relatifs aux **clauses de contrats** d'informatique en nuage qui portent sur divers points traités plus haut (Lifshitz, 2011) et (Percival, 2011) :

- *Intégrité des données* – La responsabilité de préserver l'intégrité et la confidentialité des données incombe en règle générale à l'utilisateur et les fournisseurs rejettent souvent toute responsabilité.
- *Propriété des données et accès* – Il est important d'indiquer que l'utilisateur possède les données et ce qu'il advient des données à la résiliation du contrat; de s'assurer que les différends sur les montants impayés ne bloquent pas les données et n'entraînent pas leur suppression; de s'assurer que les données sont accessibles et utilisables en cas d'interruption, de litige ou de faillite et de s'entendre à l'avance sur le format des données et les frais de récupération.
- *Licences* – Les utilisateurs doivent s'assurer qu'il existe une méthode adéquate d'octroi de licences pour utiliser la PI et le contenu accessible; faire attention au fait qu'il existe un risque accru d'infraction à la PI dans les situations où les compétences sont multiples.
- *Limites des représentations, des garanties et de la responsabilité* – les contrats d'informatique en nuage rejettent souvent toute garantie en matière de qualité de leurs services ou d'interruption de service, ce qui peut entraîner la perte de données; les limites de responsabilité générales sont courantes et doivent être évitées.
- *Indemnités* – Ces clauses sont souvent aussi générales et elles favorisent toujours le fournisseur d'informatique en nuage; les utilisateurs doivent trouver des solutions en cas de plaintes de tiers si le logiciel fourni porte atteinte à leurs droits de PI.
- *Compétence* – Il peut s'agir là d'un problème pour la résolution de différends; les lois sur le contrôle des exportations peuvent être un facteur, l'emplacement des données doit être clairement indiqué.
- *Accords sur les niveaux de service (ANS)* – Les ANS emploient souvent un vocabulaire vague et des définitions très précises quant aux garanties de service et à l'accès aux statistiques sur la qualité des services; il est important de demander le droit de vérifier les niveaux de service.
- *Perte de données* – L'inaccessibilité aux données en cas d'interruption du service peut ne pas constituer une panne selon les termes des ANS; il faut déterminer clairement qui est responsable des coûts de reproduction des données et de l'indemnisation pour les données perdues ou supprimées.
- *Conservation des données* – Les lois ou les règlements peuvent ordonner la conservation des données pendant une certaine période à certains endroits; il faut s'entendre sur les politiques de conservation et de destruction des données.
- *Protection des renseignements personnels* – La politique sur la protection des renseignements personnels du fournisseur d'informatique en nuage doit stipuler que les renseignements personnels sont conservés sur le nuage; la conformité avec la LPRPDE doit figurer dans les contrats; étant donné que la LPRPDE ne protège pas les secrets professionnels et d'autres renseignements exclusifs (à moins qu'ils contiennent des renseignements personnels), les contrats doivent correctement traiter ces éléments; envisager des clauses particulières dans les contrats sur des avis obligatoires en cas d'atteinte aux données et sur l'indemnisation en cas d'accès, d'utilisation, de divulgation ou de transfert inadaptés des renseignements personnels.

PLANIFICATION D'UNE ENQUÊTE ÉLECTRONIQUE

Il est conseillé d'établir un plan d'enquête électronique entre l'utilisateur et le fournisseur d'IN, qui comporte les éléments suivants (Selznick, 2011) :

- **Une équipe d'intervention d'enquête électronique composée de personnes désignées du fournisseur et des organismes utilisateurs, et d'un conseiller juridique;**
- **Définition du rôle du fournisseur dans l'enquête électronique;**
- **Détails sur les éléments suivants :**
  - **types de données conservées et les lieux d'entreposage**
  - **méthode d'accès aux données**
  - **procédures d'indexation et de recherche des données**
  - **procédures pour mettre en évidence une chaîne de possession claire des données en question**
  - **délais d'exécution pour la séparation des données**
  - **procédures de conservation et d'accès**
  - **capacité du fournisseur à sous-traiter**
  - **questions de succession**

- *Sécurité* – Les problèmes peuvent viser les mesures de sécurité matérielle, opérationnelle ou des programmes des fournisseurs d'informatique en nuage; il y a en règle générale un grand secret autour des capacités des fournisseurs en ce qui a trait à la sécurité; les fournisseurs s'engagent généralement à respecter un ensemble de normes et de processus pour atténuer les atteintes à la sécurité, mais ils ne garantissent pas qu'il n'y aura pas d'atteintes; diviser les responsabilités entre votre administrateur et celui du fournisseur d'informatique en nuage afin qu'aucune organisation n'ait d'accès libre à l'ensemble des couches de sécurité.
- *Vérifications, certifications et inspections* – Les utilisateurs doivent demander un droit d'effectuer des vérifications; les certifications doivent reposer sur les normes ISO 27001 ou SAS70; exiger la transparence des programmes de gestion de la poursuite des activités et de la sécurité.
- *Modification de contrats* – Cherchez les conditions qui permettent au fournisseur de modifier unilatéralement les conditions générales du contrat ou d'imposer la résiliation du contrat d'après des critères que lui seul détermine.
- *Résolution de différends* – Les utilisateurs doivent se renseigner sur la façon dont les différends sont réglés et sur le processus de recours à la hiérarchie en cas de problème; le mode alternatif de règlements des conflits (MARC) est un outil utile en présence de plusieurs compétences.

3.4.2 Enquête électronique et litige

Les organisations qui envisagent d'utiliser des services d'informatique dans le nuage doivent également tenir compte des procédures et des systèmes de conservation de documents et de données qui appuient la préparation aux **litiges**, ainsi que les stratégies pour déterminer et défendre les processus d'enquête électronique (Selznick, 2011). Il est important que les utilisateurs potentiels d'informatique en nuage sachent que la relation avec le fournisseur d'informatique en nuage, les conditions de l'entente de service et l'architecture des systèmes du fournisseur peuvent avoir de fortes conséquences sur la détermination des pouvoirs, la possession et le contrôle des données, dans le cadre des enquêtes juridiques. Les utilisateurs doivent s'assurer que la formulation des contrats d'informatique en nuage est claire afin qu'ils puissent respecter leur obligation juridique de produire des documents en cas de litige (p. ex. processus de conservation adéquats, méthodes et processus de sélection de recherche réactifs, etc.)

Lorsque les choses tournent mal, on a souvent recours à l'informatique judiciaire pour savoir ce qui s'est passé, savoir quelles sont les portions du système qui sont touchées, découvrir comme éviter de tels incidents à l'avenir et prélever des renseignements en cas d'éventuelles poursuites judiciaires. Ces preuves peuvent être plus compliquées dans un environnement d'informatique en nuage.

PREUVES INFORMATIQUES DANS LE NUAGE

Les preuves informatiques sont plus compliquées dans le nuage pour les raisons suivantes :

- **La façon dont les responsabilités en matière de gestion des incidents sont définies dans les ANS**
- **Si les horloges sont synchronisées ou pas entre les centres de données pour aider à reconstruire la chaîne d'événements**
- **La façon dont les lois sur les avis d'atteinte aux données sont appliquées dans les différents pays**
- **Les données qu'un fournisseur de nuage peut consulter lorsqu'il prend une image d'un disque dur partagé**
- **Ce que l'utilisateur peut voir dans le rapport de vérification (p. ex. les données liées à d'autres abonnés du nuage sont-elles protégées?)**
- **Si l'utilisateur est tenu de signaler un incident dans un modèle PaaS**
- **Si le fournisseur a le droit d'intervenir pour arrêter une attaque dans une application de son nuage s'il s'agit uniquement d'une relation contractuelle indirecte (p. ex. trois niveaux de clients)**

3.4.3 Questions relatives aux compétences juridiques

Bon nombre des questions juridiques entourant l'informatique en nuage sont des questions de **compétence**, et un récent livre blanc publié par Fasken Martineau démystifie plusieurs idées fausses liées aux compétences[2] (Kyer et Stern, 2011) :

- *Mythe 1 : Le choix de clauses juridiques résout le dilemme des compétences* – Le choix de lois ne signifie pas qu'on traitera les actes délictuels présumés en vertu de la loi en question, qu'on évaluera la propriété intellectuelle créée par les parties en vertu de la loi ou qu'on déterminera les lois de protection des consommateurs d'après ce choix.
- *Mythe 2 : Il existe des règles distinctes pour déterminer les compétences dans le cyberespace* – On a adopté certaines lois spéciales pour Internet, mais la règle générale est que cette méthode d'activité est assujettie aux mêmes règles et principes généraux que les autres méthodes d'activités qui comportent un aspect international ou qui englobent plusieurs compétences.
- *Mythe 3 : La compétence pour le commerce électronique est déterminée en fonction du lieu où se trouve le serveur* – Cette méthode peut ou non être un élément pertinent à prendre en compte pour déterminer la compétence, mais même si c'était vrai, dans le cas de l'informatique en nuage, il est difficile de déterminer une fois pour toutes où se trouvent les serveurs pertinents.
- *Mythe 4 : Il existe un seul ensemble de règles pour déterminer la compétence* – Il n'existe pas une seule loi internationale applicable ni un ensemble de règles et de principes qui s'appliquent à l'échelle internationale. À l'instar du Canada, bon nombre de pays renferment plusieurs compétences (nous n'avons pas une seule méthode en matière de conflit de lois). Même lorsqu''il n'y a qu'une compétence, il existe souvent des règles et des principes distincts qui visent les conflits dans les contrats, les actes délictuels, la protection des consommateurs, etc.

[2] Le document traite ensuite de l'identification et de la gestion des risques liés aux compétences multiples

3.5 Archivage et conservation

Comme il est indiqué dans la section précédente, certaines questions juridiques sont étroitement liées aux problèmes de **conservation** des données dans le nuage. Par exemple, il peut y avoir des exigences juridiques relatives à la conservation des données pendant des périodes prolongées à certains endroits, mais la conservation peut être difficile à assurer dans le nuage (p. ex. les cadres temporels de conservation peuvent dépasser les conditions générales de l'ANS, il peut être difficile de télécharger des données dans des conditions rigoureuses et il peut y avoir des modifications ou des éliminations de données programmées). Les utilisateurs doivent eux-mêmes protéger les données en s'assurant que les fournisseurs de services informatiques savent ce qu'il faut conserver et qu'ils puissent continuer d'entreposer ces données aussi longtemps qu'il le faut. Comme il est également indiqué plus haut, les exigences en matière d'enquête électronique stipulent que les parties d'un contrat de service d'informatique dans le nuage doivent aussi s'assurer qu'il existe des processus adéquats pour défendre la valeur et la crédibilité de tout document à produire.

Un autre problème qui se présente avec l'informatique en nuage est l'éventuelle **séparation** d'autres types de données (p. ex. clips vidéo, photo, courriel, données de cartographie, etc.) entre différents fournisseurs de services d'informatique en nuage. Cette dispersion des données fait en sorte qu'il est beaucoup plus difficile de trouver tous les renseignements sur un sujet précis, par exemple, dans une loi sur l'accès à l'information (loi fédérale) ou sur la liberté de l'accès à l'information (loi provinciale). DuraCloud offre une solution pour surmonter cette difficulté de conservation et d'archivage. Il s'agit d'un outil à source ouverte qui permet aux utilisateurs d'informatique en nuage de faire autant de copies de leur contenu qu'ils le souhaitent et de conserver ces copies auprès de plusieurs fournisseurs d'entreposage de données différents dans le nuage. L'application intègre directement les fournisseurs d'entreposage dans le nuage, aide à synchroniser automatiquement les copies et permet aux utilisateurs de vérifier la santé de l'ensemble de leur contenu en tout temps (DuraSpace, 2012).

Les utilisateurs d'informatique en nuage pourront également tirer profit à l'avenir d'un projet de recherche mené en Europe, TIMBUS, qui examine les questions de conservation et d'accès futur aux données dans un environnement d'informatique en nuage. Le projet s'achèvera en 2014 (Kepes, 2011).

3.6 Règlementation et normes

3.6.1 Règlements

Le respect d'une multitude de règles et de **règlements** entre plusieurs compétences peut s'avérer particulièrement difficile dans le nuage. Étant donné que très peu de règlements ont été élaborés spécialement pour cet environnement,

EFFETS DES NORMES

En l'absence d'importantes normes relatives à l'informatique en nuage, le client pourra devenir dépendant de son fournisseur. Dans le cas de l'Ordnance Survey, il a fallu modifier l'application pour utiliser certaines fonctions du service de nuage d'Amazon, ce qui a en effet lié l'organisme à Amazon.

L'Ontario GeoPortal a choisi d'utiliser les meilleures technologies et composantes et d'avoir une architecture axée sur les services pour maximiser l'interopérabilité. L'Ontario GeoPortal doit également respecter les normes internes en TI du gouvernement ontarien en matière de gestion des comptes, de sécurité, etc.

il peut s'avérer difficile pour un utilisateur de l'informatique en nuage de prouver que son organisation respecte les règles en l'absence d'une stratégie fondée sur une compréhension détaillée de l'interaction entre l'environnement de réglementation et l'informatique en nuage. Les règlements peuvent limiter l'éventail d'options dans le nuage qui s'offrent à une organisation, car celle-ci peut être obligée de respecter des règlements sur la poursuite des activités et le rétablissement après une catastrophe, les normes de sécurité (ISO 27001), les registres et les historiques d'expertise ainsi que les normes précises et les exigences de conformité gouvernementale comme celles de l'Industrie des cartes de paiement (PCI), de la *Health Insurance Portability and Accountability Act* (HIPAA) des États-Unis et de la LPRPDE au Canada. Afin que les organisations respectent les divers règlements, elles pourraient avoir à adopter une solution communautaire hybride ou dans le nuage, et éventuellement perdre tous les avantages de l'utilisation du nuage.

3.6.2 Normes

Les clients se soucient surtout du prix, de la sécurité, de l'accessibilité et de la fonctionnalité des caractéristiques, mais les **normes** peuvent également être importantes. Par exemple, sans norme, dans la communauté du nuage, les clients peuvent être « dépendants » du fournisseur de services qu'ils ont choisi parce que leur configuration ne serait pas transportable d'un fournisseur de nuage à l'autre, même s'ils souhaitent ou doivent changer. Toutefois, malgré l'immaturité relative de l'informatique en nuage, la reconnaissance de l'importance des normes a donné naissance à un éventail d'activités et d'organes de création de normes relatives à l'informatique en nuage, comme l'illustre la Figure 7 (Cloud-Standards.org, 2010).

Figure 7 : Organisations participant à la création de normes relatives à l'informatique en nuage

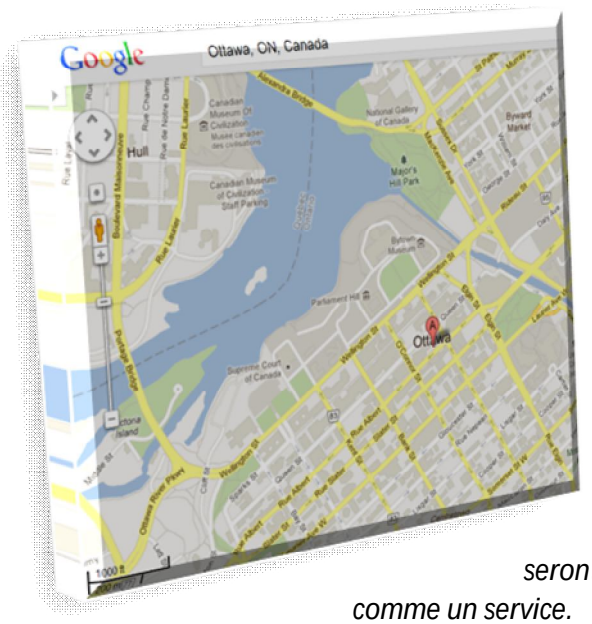
Quelques initiatives clés de ces organisations :

- Le National Institute of Standards and Technology (NIST) détermine les lacunes des normes et spécifications liées au nuage et publie les lacunes sur son portail.
- La Cloud Security Alliance (CSA) réalise plusieurs initiatives et propose des outils pour aider les utilisateurs et les fournisseurs de nuage à évaluer et à adopter l'informatique en nuage.
- Le Telecommunications Standard Sector [Secteur des normes de télécommunication] de l'Union internationale des télécommunications (ITU-T) a mis sur pied un groupe de consultation sur l'Informatique en nuage chargé de contribuer aux aspects de l'informatique en nuage qui utilisent les réseaux de télécommunication.
- L'Open Management Group se concentre sur les modèles de déploiement d'applications et de services dans les nuages en ce qui a trait à la portabilité, l'interopérabilité et la réutilisation.
- L'IEEE Computer Society travaille sur les normes relatives à l'informatique en nuage afin d'aider à favoriser la portabilité et à accroître l'interopérabilité.

L'Open Geospatial Consortium (OGC), le principal organisme d'établissement de normes dans le domaine géospatial, affirme que ses normes et l'architecture connexe sont compatibles avec le nuage, étant donné qu'elles sont conçues pour permettre l'interopérabilité entre les plateformes, y compris le nuage (Ramage, 2011). Toutefois, d'après une analyse comparative de trois plateformes de PaaS menée par des chercheurs de l'Université de Pretoria, il existe certains problèmes potentiels de sécurité (p. ex. fichiers malveillants sur les machines d'hébergement et attaques entraînant un refus de service (ARS) pendant la conception d'un service de traitement Web dans un nuage PaaS (Ludwig et Coetzee, 2010).

4. Conséquences, avantages et risques

4.1 Conséquences sur l'infrastructure de données géospatiales du Canada et ses intervenants



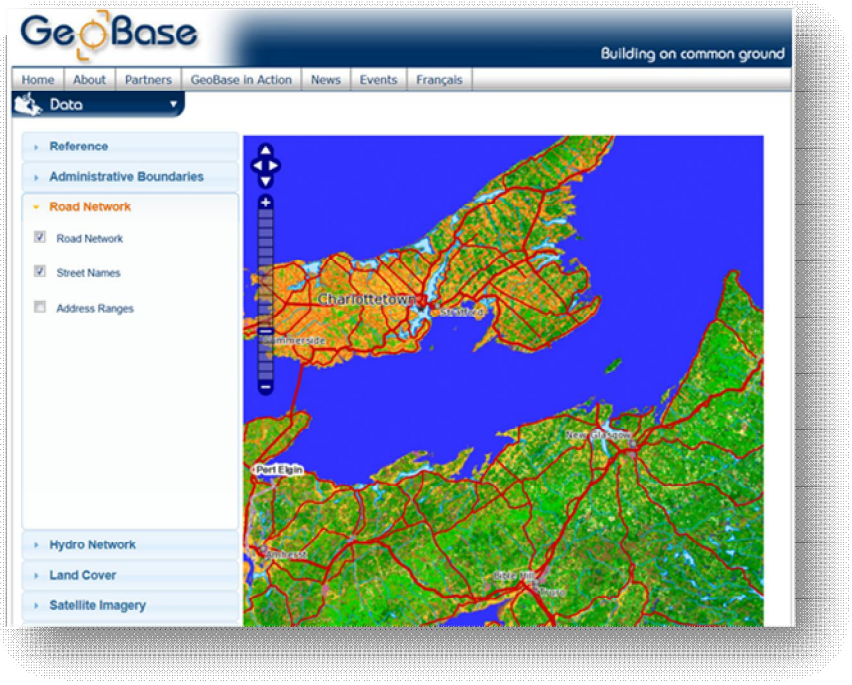
À mesure qu'un nombre croissant de solutions d'informatique en nuage géospatiale feront leur apparition, il sera essentiel de satisfaire aux besoins fondamentaux en matière de données de base ou cadre. La plupart des solutions d'informatique en nuage commercialisées ne comportent pas de données. Cependant, dans le cas des solutions cartographiques, on a toujours besoin de données géospatiales, et il existe un ensemble de données de base dont presque tous les clients ont besoin. De plus, la plupart des clients du nuage n'ont pas les capacités techniques ou le personnel requis pour bâtir, acquérir et/ou tenir à jour leurs propres données géospatiales de base. Ils *espéreront donc que ces données seront accessibles comme un service.*

Les grands acteurs commerciaux qui ont lancé des services de cartographie et d'imagerie, comme Google Maps et Bing Maps, respectent en grande partie les exigences de la communauté de clients en ligne en matière de données géospatiales de base, en fournissant des références de localisation visuelles et une fonctionnalité géospatiale de base. Cependant, en règle générale, ils ne traitent pas les besoins en matière de données thématiques portant notamment sur la gestion des ressources, l'agriculture, l'environnement, la démographie, l'économie, l'éducation, etc. Lorsqu'un plus grand nombre de clients utilisera les cartes à des fins d'affichage, d'autres fonctions de traitement seront requises.

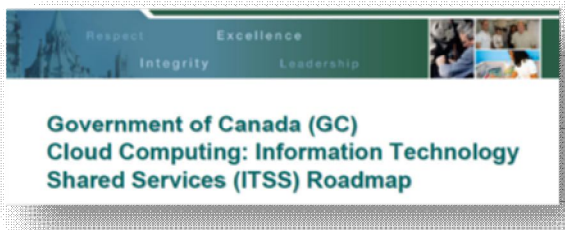
L'infrastructure de données spatiales du Canada doit être prête afin de tirer profit de ces tendances et d'y répondre, à savoir l'augmentation des besoins en données géospatiales et la hausse de l'utilisation de la fonction géospatiale. L'ICDG peut jouer un rôle essentiel pour appuyer l'évolution et l'adoption de l'informatique en nuage géospatiale, particulièrement dans cette communauté croissante d'utilisateurs qui n'ont pas d'expérience ni d'aptitudes dans le domaine géospatial, en étant une source de :

a) données géospatiales – accompagnées de renseignements sur les caractéristiques – qui sont facile à acquérir et à utiliser dans une application en ligne;
b) fonction géospatiale qui peut être intégrée dans les solutions SaaS.

Les services de cartographie qui sont accessibles par le biais de l'ICDG comme GéoBase n'ont pas besoin de faire concurrence aux fournisseurs de données de base commerciaux. Il y a encore une forte demande à l'égard des services pour qu'ils fournissent des données de base faisant autorité que les agences géospatiales gouvernementales rendent accessibles par le biais de l'infrastructure de données spatiales. L'ICDG trouvera également de nouvelles façons de fournir des services de données thématiques, particulièrement lorsque les données géospatiales seront très utilisées et que le nuage deviendra une méthode convenable pour les applications qui appuient son utilisation.



On réfléchit sérieusement à l'adoption de l'informatique en nuage à l'échelle fédérale, comme il est indiqué à la Section 1. D'après les observations, les provinces analysent elles aussi activement le potentiel de l'informatique en nuage. Les organisations gouvernementales d'information géospatiale feront partie des instances les plus touchées, compte tenu de la taille de leurs ensembles de données et ils devront évaluer l'ensemble des questions de politiques opérationnelles abordées aux présentes lorsqu'ils prépareront des plans de migration vers le nuage. Les fournisseurs de données du secteur privé du Canada qui adoptent le nuage devront également évaluer les enjeux relatifs aux politiques opérationnelles abordés aux présentes. Ils devront porter une attention particulière aux questions juridiques comme la protection des renseignements personnels et la confidentialité ainsi que l'octroi de licences. Les intervenants de l'ICDG tentent déjà de trouver comment conserver et archiver au mieux les données géospatiales numériques pour la recherche et en cas d'éventuelles enquêtes électroniques et la migration des données vers le nuage compliquera encore les choses.



Source : ITSS (Gouvernement du Canada, 2010)

4.2 Avantages

En plus des avantages couramment associés à l'informatique en nuage, l'*informatique en nuage géospatiale* offre les avantages *supplémentaires* suivants :

- *Faible coût de mise en œuvre* – acquisition d'un service, pas de logiciel serveur, données spatiales et hébergement.
- *Certitude accrue* – faible risque; l'ING aide à simplifier ce qui en règle générale est assez complexe.
- *Données géospatiales* – gestion et accessibilité.
- *Capacité* – mise en œuvre possible sans expertise en SIG.

Par extension, l'informatique en nuage peut avoir des effets bénéfiques sur l'ICDG et ses intervenants. Lorsque de nouvelles options commerciales d'informatique en nuage géospatiale feront leur apparition sur le marché, les organisations qui ont peu ou pas d'expérience en solutions géospatiales auront moins d'obstacles à surmonter pour adopter cette puissante technologie. La croissance qui en résultera dans la communauté d'utilisateurs augmentera la demande en matière de données géospatiales de haute qualité de toutes sortes, ce qui prouvera encore plus la valeur des données rendues accessibles par le biais de l'ICDG. L'accès à des données géospatiales par le biais de services Web augmentera lorsque la demande des utilisateurs passera des organisations professionnelles du secteur géospatial qui téléchargent généralement des données dans leurs propres systèmes de SIG à la consommation de données par un bien plus large éventail d'organisations, en fonction de leurs besoins. Les intervenants de l'ICDG devront s'efforcer de satisfaire au quotidien à la demande de volume élevé d'accès Web aux correctifs de données.

4.3 Risques

Au gré de l'évolution de la technologie et de la capacité des services ainsi que de l'infrastructure Internet sous-jacente, les principaux risques associés à l'informatique en nuage sont en règle générale liés aux questions de politiques opérationnelles abordées aux présentes. Toutefois, il faut également tenir compte d'un grand risque technologique pour les intervenants de l'ICDG. Comme il est indiqué dans la section précédente, la consommation de données géospatiales par le biais de services Web de haute qualité devrait augmenter rapidement. La capacité actuelle de l'ICDG et des organisations d'intervenants qui fournissent l'accès à leurs données par le biais de l'infrastructure pour satisfaire à cette demande est limitée. On a adopté des normes relatives au service Web (WMS, WFS, etc.), mais l'accès aux données par le biais de l'ICDG se fait encore en grande partie par le biais du téléchargement de données. Si l'on ne corrige pas cette faiblesse de l'infrastructure, les fournisseurs de données commerciaux remédieront à cette incapacité de l'ICDG à fournir efficacement des données pour les applications de l'informatique en nuage géospatiale.

La migration des composantes matérielles et logicielles de l'ICDG (ou d'autres infrastructures de données spatiales (IDS) au Canada) vers le nuage aura de nombreuses conséquences. Par exemple, l'absence de normes sur l'informatique en nuage reconnues à l'échelle internationale pourrait poser des problèmes de compatibilité avec l'IDS, qui est axée sur des normes. Bien que les normes de l'OGC adoptées pour l'ICDG visent à exploiter les environnements dans le nuage, comme l'indique la Section 3.6.2, il y aurait, d'après certaines recherches, des problèmes liés aux services de traitement Web dans le nuage. L'absence de normes sur l'informatique en nuage a également des conséquences sur l'interopérabilité entre les données/applications dans les différentes solutions du nuage et peut entraîner une dépendance exclusive à un fournisseur. Cette situation peut avoir des répercussions sur

les activités de l'IDS ainsi que sur la durabilité de certaines composantes de l'IDS dans le nuage si un fournisseur met fin à ses activités ou prend une orientation très différente incompatible avec le modèle de l'IDS. Il faudra des évaluations très pertinentes sur la sécurité provenant des fournisseurs d'informatique en nuage pour bien choisir entre les nuages publics, privés, communautaires ou hybrides afin de veiller à la protection des données privées, confidentielles et sensibles accessibles par l'entremise de l'ICDG.

Il sera difficile pour les intervenants de l'ICDG de résoudre ces problèmes liés aux politiques opérationnelles, mais les expériences présentées dans les deux études de cas (Ordnance Survey et Ontario GeoPortal) montrent qu'ils pourront y parvenir.

5. Conclusions

L'utilisation de l'informatique en nuage par des organisations des secteurs publics et privés augmente rapidement et les organisations du secteur de l'information géospatiale adoptent ce nouveau modèle informatique également. L'informatique en nuage offre de nouvelles façons de fournir des données géospatiales, des logiciels et une infrastructure informatique comme des services en ligne, et réduit ainsi les obstacles liés à l'utilisation de cette puissante technologie par les non-professionnels du SIG.

Le présent document vise à mettre en évidence les principaux enjeux relatifs aux politiques opérationnelles auxquels les organisations qui travaillent avec l'informatique en nuage doivent faire face – particulièrement en ce qui a trait à la sécurité des données, à la protection des renseignements personnels et à la confidentialité, aux questions juridiques, d'archivage et de conservation, aux règlements et aux normes. Les renseignements fournis sur les politiques et les méthodes en vigueur ainsi que les principales leçons tirées par les personnes chargées de la mise en œuvre de l'informatique en nuage fourniront de l'orientation à quiconque souhaite mettre en œuvre ou améliorer sa propre solution d'informatique en nuage.

Annexe 1 : Glossaire

Acronyme	Terme	Définition
MARC	Mode alternatif de règlements des conflits	Processus que l'on peut utiliser pour régler un conflit, un différend ou une plainte qu'un tribunal prenne une décision pendant un procès ou que d'autres institutions prennent une résolution relative à une affaire ou un contrat (American Bar Association Section of Dispute Resolution, 2006).
	Application	Logiciel conçu pour aider l'utilisateur à réaliser des tâches données.
API	Interface de programmation d'applications	Instruction liée au code source (p. ex. pour des routines, des structures de données, des catégories d'objets et des variables) conçue pour être utilisée comme interface par les composantes logicielles pour communiquer entre elles.
	Archivage	Recueil des documents historiques (c.-à-d. documents retenus à des fins de conservation permanente ou à long terme en vertu de leur valeur culturelle, historique ou probante)
ICDG	Infrastructure canadienne de données géospatiales	L'ICDG révèle de nouvelles perspectives aux Canadiens à l'égard de questions sociales, économiques et environnementales, en fournissant un réseau de ressources en ligne qui permet d'améliorer le partage et l'utilisation d'information liée à des lieux géographiques du Canada.
IN	Informatique en nuage	Modèle qui permet d'offrir un accès au réseau généralisé sur demande à un ensemble partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, entreposage, applications et services) qui peuvent rapidement être fournies et diffusées en requérant un effort de gestion minime ou peu d'interaction du fournisseur de service.
	Informatique judiciaire	Techniques d'enquête et d'analyse informatiques visant à trouver des preuves légales. (Lexbe.com , 2012)
	Renseignements confidentiels	Renseignements qu'il faut garder secrets au sein d'un cercle de personnes et qui ne doivent pas être connus du public. Accessibles uniquement aux personnes autorisées.
	Droit d'auteur	Droit exclusif de produire ou de reproduire une œuvre ou toute partie importante d'une œuvre sous n'importe quelle forme matérielle qui soit ou droit d'autoriser ces actions.
ARS	Attaque entraînant un refus de service	Attaque d'un ordinateur où l'attaquant tente d'empêcher les utilisateurs autorisés à accéder aux données ou aux services comme la messagerie électronique, les sites Web, les comptes

Acronyme	Terme	Définition
		en ligne (bancaires, etc.) ou d'autres services qui requièrent l'ordinateur touché (US-CERT, 2009).
	Enquête électronique	Collecte, préparation, examen et production de documents électroniques pendant les enquêtes en cas de litige. Englobe les courriels, les pièces jointes et d'autres données conservées sur un ordinateur, un réseau, une copie de secours ou d'autres supports d'entreposage, ainsi que les métadonnées. (Lexbe.com, 2012)
ING	Informatique en nuage géospatiale	L'ING peut être considérée comme un service dans le nuage qui englobe des cartes et l'utilisation et la manipulation de données spatiales.
HIPAA	*Health Insurance Portability and Accountability Act*	Loi américaine régissant l'utilisation de renseignements personnels sur la santé.
	Infrastructure	Traitement, entreposage, réseaux et autres ressources informatiques fondamentales.
	Responsabilité	Responsabilité légale d'une personne pour ses actions ou ses omissions; en n'assumant pas sa responsabilité, une personne peut s'exposer à une poursuite judiciaire pour tout dommage qui en résulte.
	Octroyer des licences	Les donneurs de licences autorisent les titulaires de licences à utiliser l'élément visé par la licence.
	Application mobile	Application logicielle conçue pour fonctionner sur les téléphones intelligents et les tablettes.
PCI	Industrie des cartes de paiement	Normes liées à la sécurité des données des cartes de paiement.
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*	Règles du gouvernement canadien liées aux responsabilités qu'un fournisseur de services doit assumer par rapport aux renseignements qu'il collecte et qu'il conserve sur les personnes.
	Protection des renseignements personnels	Capacité d'une personne ou d'un groupe à s'isoler ou à isoler des renseignements sur lui et ainsi de se révéler de façon sélective.
	Naturellement	Façon dont la capacité de traitement ou d'entreposage est ajoutée ou supprimée sans mesure délibérée de l'utilisateur ou même sans qu'il sache qu'une telle modification a lieu.
	Sécurité	Moyens de protéger les renseignements qui se trouvent sur les ordinateurs, du vol, de la corruption ou des catastrophes naturelles qui permettent de faire en sorte que les données restent accessibles et productives pour les utilisateurs ciblés.
ANS	Accord sur les niveaux de service	Contrat entre un fournisseur de services et un client qui stipule une compréhension commune des services, des priorités, des responsabilités, des garanties et qui présente en détail la nature,

Acronyme	Terme	Définition
		la qualité et la portée du service à fournir, en règle générale dans des termes mesurables.
	Acte délictuel	Délit civil, autre qu'une rupture de contrat, auquel la loi remédiera en accordant des dommages-intérêts. (Canada Legal Information Sources, 2012)
	Navigateur Web	Application logicielle permettant de récupérer, présenter et explorer des ressources d'information dans le Web.

Annexe 2 : Références

American Bar Association Section of Dispute Resolution, *What You Need to Know about Dispute Resolution: The Guide to Dispute Resolution Processes*, 2006. Consulté le 15 février 2012, sur le site Web de l'American Bar Association [http://www.americanbar.org/content/dam/aba/migrated/2011_build/dispute_resolution/draftbrochure.authcheckdam.pdf]

Badger, L., T. Grance, R. Patt-Corner et J. Voas, *DRAFT Cloud Computing Synopsis and Recommendations : Recommendations of the National Institute of Standards and Technology*, mai 2011. Consulté le 28 décembre 2011, sur le site Web du NIST [http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf]

Bailey, S., *Data Preservation and Retrieval*, avril 2010. Consulté le 12 janvier 2012, sur le site Web de JISC infoNet [http://www.jiscinfonet.ac.uk/infokits/cloud-computing/information-management]

Bradshaw, S. C. Millard et I. Walden, 1er septembre 2010, « Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services ». Consulté le 3 mars 2012, sur le site Web du Social Science Research Network [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374##]

Canada Legal Information Sources, *Introduction to "What is a TORT CLAIM? How is this related to expenses from personal injuries?*, 2012. Consulté le 16 février 2012, sur le site Web de Canada Legal Information Sources [http://www.canadalegal.info/prov-bc/0-ref-library/personal-injury/personal-injury-bc-icbc-03.html]

Cloud Security Alliance, *Security guidance for critical areas of focus in cloud computing v3.0*, 2011. Consulté le 2 janvier 2012, sur le site Web de Cloud Security Alliance [https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf]

Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*, mars 2010. Consulté le 5 janvier 2012, sur le site Web de Cloud Security Alliance [https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf]

Cloud-Standards.org, *Cloud Standards Overview*, 17 mai 2010. Consulté le 2 janvier 2012, sur le site Web de Cloud-Standards.org [http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview]

Corley, R., « Negotiating and drafting cloud computing contracts: a checklist for cc deals », *Cloud Computing Law Workshop.* Toronto, Federated Press, 2011.

Danek, J., *Government of Canada (GC) Cloud Computing: Information Technology Shared Services (ITSS) Roadmap,* avril 2010. Consulté le 23 janvier 2012, sur le site Web du Conseil consultatif canadien sur les normes de TIC [http://www.isacc.ca/isacc/_doc/ArchivedPlenary/ISACC-10-43305.pdf]

Drake, J., A. Jacob, N. Simpson et S. Thompson, *Open Data Center Alliance Developing Cloud-Capable Applications White Paper*, novembre 2011. Consulté le 30 décembre 2011, sur le site Web de l'Open Data Center Alliance [http://www.opendatacenteralliance.org/docs/Best_Practices_whitepaper.pdf]

DuraSpace, *Preservation and Archiving*, 2012. Consulté le 12 janvier 2012, sur le site Web de DuraCloud [http://www.duracloud.org/preservation_and_archiving]

Escalante, D. et A. J. Korty, *Cloud Services : Policy and Assessment*, juillet 2011. Consulté le 28 décembre 2011, sur le site Web d'Educause Review, vol. 46, n° 4 [http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume46/CloudServicesPolicyandAssessme/231833]

Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), *Cloud Computing Information Assurance Framework*, novembre 2009. Consulté le 3 janvier 2012, sur le site Web de l'ENISA [http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework?searchterm=Cloud+Computing+Information+Assurance+Framework]

Gellman, R., *Privacy in the Clouds : Risks to Privacy and Confidentiality from Cloud Computing*, 23 février 2009. Consulté le 23 décembre 2011, sur le site Web du World Privacy Forum [http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf]

Gellman, R. et P. Dixon, *Cloud Computing Privacy Tips*, 23 février 2009). Consulté le 23 décembre 2011, sur le site Web du World Privacy Forum [http://www.worldprivacyforum.org/pdf/WPF_Cloud_Tips_fs.pdf]

Gens, F., *New IDC IT Cloud Services Survey : Top Benefits and Challenges*, 15 décembre 2009. Consulté le 15 décembre 2011, sur le site Web d'IDC exchange [http://blogs.idc.com/ie/?p=730]

Jackson, K. L. *It's Official! US Intelligence Community Is Moving To The Cloud!*, 17 octobre 2011. Consulté le 15 décembre 2011, sur le site Web de Forbes.com [http://www.forbes.com/sites/kevinjackson/2011/10/17/its-official-us-intelligence-community-is-moving-to-the-cloud/]

Karn, B., *Data Security — The Case Against Cloud Computing*, 31 mars 2011. Consulté le 2 janvier 2012, sur le site Web de casselsbrock.com [http://www.casselsbrock.com/files/file/docs/Data%20Security%20-%20The%20Case%20Against%20Cloud%20Computing%20PDF.pdf]

Kepes, B., *New EU Digital Preservation Project*, 19 septembre 2011.Consulté le 23 janiver 2012, sur le site Web de CloudAve [http://www.cloudave.com/14995/new-eu-digital-preservation-project/]

Kyer, C. I., G. M. Stern, *Where in the World is My Data? Jurisdictional Issues with Cloud Computing*, 30 mars 2011. Consulté le 2 janvier 2012, sur le site Web de Fasken Martineau [http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/aea8833f-ab3c-48f1-854d-6ec4be989775/Jurisdictional_Issues_with_Cloud_Computing_Ian_Kyer_Gabriel_Stern.pdf]

Lexbe.com, *e-Discovery & Metadata Definitions*, 2012. Consulté le 16 février 2012, sur le site Web de Lexbe.com [http://www.lexbe.com/hp/define-e-Discovery-metadata.htm]

Lifshitz, L. R. « Understanding Cloud Computing: Legal Issues and Best Practices », *Loud Computing Law, Toronto : Federated Press*, 2011.

Ludwig, B. et S. Coetzee, *A Comparison of PaaS Clouds with a Detailed Reference to Security and Geoprocessing Services*, 26 août 2010. Consulté le 23 décembre 2011, sur le Web [http://webmgs2010.como.polimi.it/presentations/2_LudwigCoetzee.pdf]

McDonald, S., « Legal and Quasi-Legal Issues in Cloud Computing Contracts »,le 2 février 2010. Consulté le 28 décembre 2011, sur le site Web d'Educause [http://net.educause.edu/section_params/conf/CCW10/issues.pdf]

Mel, P. et T. Grance, *The NIST Definition of Cloud Computing*, septembre 2011. Consulté le 20 décembre, 2010, sur le site Web du National Institute of Standards and Technology [http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf]

Messmer, E., *Best security questions to ask about SaaS*, 12 mars 2009. Consulté le 15 décembre 2011, sur le site Web de Network World [http://www.networkworld.com/news/2009/031209-saas-security.html]

Microsoft, *Ontario Government Sees Waves of Potential After Testing Private Cloud Solution*, 11 juillet 2011. Consulté le 23 janvier 2012, sur le site Web de Microsoft Case Studies [http://www.microsoft.com/casestudies/Case_Study_Detail.aspx?CaseStudyID=4000011335]

NEC; CIPVP Ontario, *Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach*, mai 2010. Consulté le 6 janvier 2012, sur le site Web du Commissaire à l'information et à la protection de la vie privée, Ontario [http://www.privacybydesign.ca/content/uploads/2010/07/pbd-NEC-cloud.pdf?search=search]

Office of the Chief Information Officer*IM/IT Enablers Strategy v1.5 for Citizens @ the Centre : BC government 2.0*, 19 juillet 2011. Consulté le 23 janvier 2012, sur le site Web de l'Office of the Chief Information Officer [http://www.cio.gov.bc.ca/local/cio/about/documents/it_strategy.pdf]

Commissariat à la protection de la vie privée du Canada, *Visez les nuages : questions liées à la protection de la vie privée dans le contexte de l'informatique dans les nuages*, 29 mars 2010. Consulté le 2 janvier 2012, sur le site Web du Commissariat à la protection de la vie privée du Canada [http://www.priv.gc.ca/information/pub/cc_201003_f.cfm#toc2c1]

Ontario GeoPortal, *Ontario GeoPortal Comparison,*1er juin 2011. Consulté le 3 mars 2012, sur le site Web d'Ontario GeoPortal [http://www.ontariogeoportal.com/Documents/OntarioGeoPortalComparison.pdf]

Open Data Center Alliance, *Open Data Center Alliance Usage : Provider Security Assurance*, 7 juin 2011a. Consulté le 2 janvier 2012, sur le site Web de l'Open Data Center Alliance [http://www.opendatacenteralliance.org/ourwork/usagemodels]

Open Data Center Alliance,*Open Data Center Alliance Usage : Regulatory Framework*, 7 juin 2011d. Consulté le 2 janvier 2012, sur le site Web de l'Open Data Center Alliance [http://www.opendatacenteralliance.org/ourwork/usagemodels]

Open Data Center Alliance, *Open Data Center Alliance Usage : Security Monitoring*, 7 juin 2011b. Consulté le 2 janvier 2012, sur le site Web de l'Open Data Center Alliance [http://www.opendatacenteralliance.org/ourwork/usagemodels]

Open Data Center Alliance, *Open Data Center Alliance Usage : Standard Units of Measure for IaaS*, 7 juin 2011e. Consulté le 2 janvier 2012, sur le site Web de l'Open Data Center Alliance [http://www.opendatacenteralliance.org/ourwork/usagemodels]

Open Data Center Alliance, *Open Data Center Alliance Usage : VM Interoperability*, 7 juin 2011c. Consulté le 2 janvier 2012, sur le site Web de l'Open Data Center Alliance [http://www.opendatacenteralliance.org/ourwork/usagemodels]

Percival, R. L., « Cloud Computing: Due Diligence Considerations ». *Cloud Computing Law Workshop, Toronto : Federated Press*, 2011.

Power, A., « Privacy Concerns with Cloud Computing », *Reventing Data Breach and Misuse Workshop, Ottawa : Federated Press*, 2011.

Ramage, S., *Standards for geospatial technology and services in cloud computing*, 5 janvier 2011. Consulté le 23 décembre 2011, sur le site Web de l'OGC [http://portal.opengeospatial.org/files/?artifact_id=42636]

Ryan, M. D., « Cloud Computing Privacy Concerns on Our Doorstep », *Communications of the ACM, Vol. 54 N^{o} 1* , pp. 36-38, 2011.

Sawyer, J., *Spot Trouble in the Cloud : Adapting Security Monitoring & Incident Response*, juin 2011. Consulté le 30 décembre 2011, sur le site Web d'InformationWeek [http://reports.informationweek.com/abstract/5/7376/Cloud-Computing/strategy-cloud-security-monitoring.html]

Selznick, S. I., « Addressing e-discovery and litigation issues », *Cloud Computing Law Workshop, Toronto : Federated Press*, 2011.

Spires, R. A., *Cloud Computing, Front and Center*, 6 septembre 2011. Consulté le 21 décembre, 2011, sur le site Web du CIO.gov [http://www.cio.gov/pages.cfm/page/Cloud-Computing-Front-and-Center]

Trend Micro, *Cloud Security Survey Global Executive Summary*, 3 juin 2011. Consulté le 15 décembre 2011, sur le site Web de Trendmicro.com [http://es.trendmicro.com/imperia/md/content/uk/about/global_cloud_survey_exec_summary_final.pdf]

US-CERT, *Understanding Denial-of-Service Attacks*, 2009. Consulté le 16 février 2012, sur le site Web de l'United States Computer Emergency Response Team [http://www.us-cert.gov/cas/tips/ST04-015.html]

Weech, M., « GIS & The Cloud », Ottawa (Ontario) Canada, 2011.

Weissberger, A., *What Should Cloud Computing Users and Providers consider for SLAs?,* 13 janvier 2011b. Consulté le 23 décembre 2010, sur le site Web de Viodi [http://www.viodi.com/2011/01/13/what-should-cloud-computing-users-and-providers-consider-for-slas/]

Weissberger, A., *Cloud Computing Issues : State of the Net West Conference – August 6, 2008, Santa Clara, CA* , 11 août 2011c. Consulté le 23 décembre 2010, sur le site Web de Viodi [http://viodi.com/2008/08/11/cloud-computing-issues-state-of-the-net-west-conference-august-6-2008-santa-clara-ca/]

Yang, C., M. Goodchild, Q. , Huang, D. Nebert, et R. Raskin, « Spatial cloud computing : how geospatial geospatial sciences could use and help to shape cloud computing », *International Journal of Digital Earth, 4:4* , 305-329, 2011.

Zients, J., *Driving IT Reform : An Update*, 19 novembre 2010.Consulté le 3 janvier 2012, sur le site Web de l'Office of Management and Budget [http://www.whitehouse.gov/blog/2010/11/19/driving-it-reform-update]

Annexe 3 : Pratiques exemplaires

La présente annexe résume les pratiques exemplaires que d'autres organisations ont adoptées pendant la mise en œuvre de l'informatique en nuage et qui pourraient intéresser les intervenants de l'ICDG.

5.1 Sécurité

La sécurité des données et des applications dans le nuage semble être le principal problème pour les utilisateurs potentiels de services d'informatique dans le nuage. La présente section porte sur les pratiques exemplaires qui aident à surmonter cet obstacle.

5.1.1 Questions de sécurité pour les fournisseurs

Quelques questions que les acheteurs potentiels de SaaS devraient poser (Messmer, 2009) :

- Quels sont les employés qui ont un accès à la racine et à la base de données et quelles sont les mesures en place pour les empêcher d'accéder aux données de votre organisation, s'il y a lieu?
- Les données conservées sont-elles chiffrées? Comment?
- Les données conservées sont-elles divisées par client, ou sont-elles toutes entreposées dans une grande base de données? Comment les données sont-elles séparées? Comment traiterez-vous la question juridique de l'enquête électronique en cas de problème opérationnel?
- Les données transférées de l'entreprise à l'infrastructure d'informatique en nuage du fournisseur sont-elles sécurisées de quelque façon que ce soit?
- Quels mécanismes empêcheront les personnes internes à l'organisation fournisseuse de télécharger vos données sur une clé USB et de les emporter?
- En termes d'accessibilité des services, votre fournisseur peut-il conclure une entente sur les niveaux de service?
- Leur centre de données se trouve-t-il dans un lieu ciblé par les ouragans ou les séismes? Quels sont leurs plans de secours?
- Quelles données sont consignées dans les registres de vérification?
- Y a-t-il moyen de limiter les endroits où le fournisseur de SaaS se rend dans le réseau d'entreprise?

Questions relatives à la sécurité que les clients doivent poser aux fournisseurs avant d'en choisir un (Brodkin, 2008) :

- Demandez aux fournisseurs de vous fournir des renseignements précis sur l'embauche et la supervision des administrateurs détenant des privilèges et sur les méthodes de contrôles qui régissent leur accès.
- Déterminer si le fournisseur de nuage consent à se soumettre à des vérifications externes et à des certifications de sécurité.

- Demandez aux fournisseurs s'ils s'engagent à entreposer et traiter les données à des endroits précis et s'ils s'engagent par contrat à respecter les exigences locales en matière de protection des renseignements personnels pour votre compte.
- Renseignez-vous sur les mesures prises pour séparer les données stockées et sur les méthodes de chiffrement prévues et testées par des spécialistes expérimentés.
- Demandez aux fournisseurs s'ils peuvent réaliser une restauration complète des données en cas de catastrophe et renseignez-vous sur le temps que prendra une telle initiative.
- Demandez aux fournisseurs de s'engager par contrat à appuyer des types particuliers d'enquêtes (p. ex. d'activité inadéquate ou illégale) et demandez-leur de vous fournir des preuves qu'ils ont déjà appuyé ce type d'activités.
- Demandez aux fournisseurs comment vous pourriez récupérer vos données si l'entreprise fait faillite ou si elle est rachetée et si elles seront dans un format que vous pouvez importer dans une application de rechange.

Yang, *et coll.* (2011) ont déterminé les éléments de base suivants en ce qui a trait à la sécurité :

- Fournisseurs d'informatique en nuage
  - veiller à la fonctionnalité et l'accessibilité des services dans le nuage
  - fournir des solutions possibles pour protéger les données contre la perte en cas de panne des services dans le nuage et prévoir des stratégies de secours en cas de panne du service dans le nuage afin de permettre le transfert des données d'un endroit à l'autre en toute sécurité
- Utilisateurs ayant des privilèges dans les entreprises d'informatique en nuage
  - séparer les fonctions liées afin d'éviter les fuites de données ou l'accès par des tiers (p. ex. les techniciens des ressources informatiques qui contrôlent l'infrastructure informatique n'ont pas accès aux comptes d'utilisateurs, tandis que le personnel chargé des comptes d'utilisateurs n'a pas accès à l'infrastructure matérielle)
- Utilisateurs finaux
  - posséder leur propre système de gestion de l'identité axé sur le niveau pour contrôler l'accès aux données et aux ressources du nuage
  - avoir uniquement un accès et un contrôle liés à leurs fonctions

5.1.2 Modèles d'utilisation sûre

L'Open Data Centre Alliance (ODCA) a conçu les modèles d'utilisation sûre suivants pour l'informatique en nuage :

- *Open Data Center Alliance Usage : Provider Security Assurance* (ODCA, 2011a) – fournit des définitions normalisées de la sécurité pour les services dans le nuage, présente en détail les moyens par lesquels les fournisseurs de services peuvent montrer leur conformité et donne aux organisations la possibilité de valider leur adhésion aux normes de sécurité dans les services dans le nuage.
- *Open Data Center Alliance Usage : Security Monitoring* (ODCA, 2011b) – fournit aux organisations utilisateurs un cadre de surveillance normalisé et des interfaces pertinentes qui leur

permettront de se renseigner sur l'état de la sécurité et de la conformité des services qu'ils reçoivent des fournisseurs.

- *Open Data Center Alliance Usage : Virtual Machine (VM) Interoperability* (ODCA, 2011c) – indique les mesures et les processus qui favorisent la création de solutions de gestion de machine virtuelle interexploitables afin de diminuer la complexité et le prix de la gestion, particulièrement dans des environnements hétérogènes où l'on trouve plusieurs fournisseurs.
- *Open Données Center Alliance Usage : Regulatory Framework* (ODCA, 2011d) – aide les organisations utilisatrices à évaluer et surveiller leurs obligations réglementaires lorsqu'ils participent aux services dans le nuage ou en font l'acquisition.

5.2 Protection des renseignements personnels

Les risques relatifs à la protection des renseignements personnels et de confidentialité arrivent juste derrière la sécurité parmi les problèmes qui découragent souvent les organisations à transférer leurs données et leurs applications vers le nuage. Les sections suivantes résument les pratiques exemplaires relevées dans la documentation pour surmonter cet obstacle.

5.2.1 Conseils destinés aux organisations et aux consommateurs d'informatique en nuage sur la protection des renseignements personnels

Les conseils suivants sur la protection des renseignements personnels dans l'informatique en nuage aideront les organisations et les consommateurs à assurer la protection des renseignements personnels (Gellman et Dixon, 2009) (Power, 2011) :

- Méfiez-vous de l'informatique en nuage « ponctuelle ». Toute organisation doit avoir des règles normalisées qui indiquent aux employés quand et s'ils peuvent utiliser l'informatique en nuage et pour quelles données.
- Ne placez rien sur le nuage que vous ne souhaitez pas qu'un concurrent, votre gouvernement, un avocat plaidant privé ou un autre gouvernement voit.
- Lisez les conditions de service et la politique sur la protection des renseignements personnels et assurez-vous de bien les comprendre.
- Assurez-vous que vous n'enfreignez pas de loi ou de politique en plaçant des données dans le nuage, et réfléchissez à deux fois avant de placer les données de vos clients dans le nuage.
- Consultez les conseillers juridique, technique ou en sécurité de votre organisation pour savoir s'il est conseillé de placer vos données dans le nuage.
- Demandez à être informé à l'avance de toute modification apportée aux conditions de service ou à la politique sur la protection des renseignements personnels.
- Assurez-vous de bien comprendre les rôles et responsabilités de chacun.
- Vérifier attentivement si le fournisseur de nuage se réserve le droit d'utiliser, de divulguer ou de publier vos données.

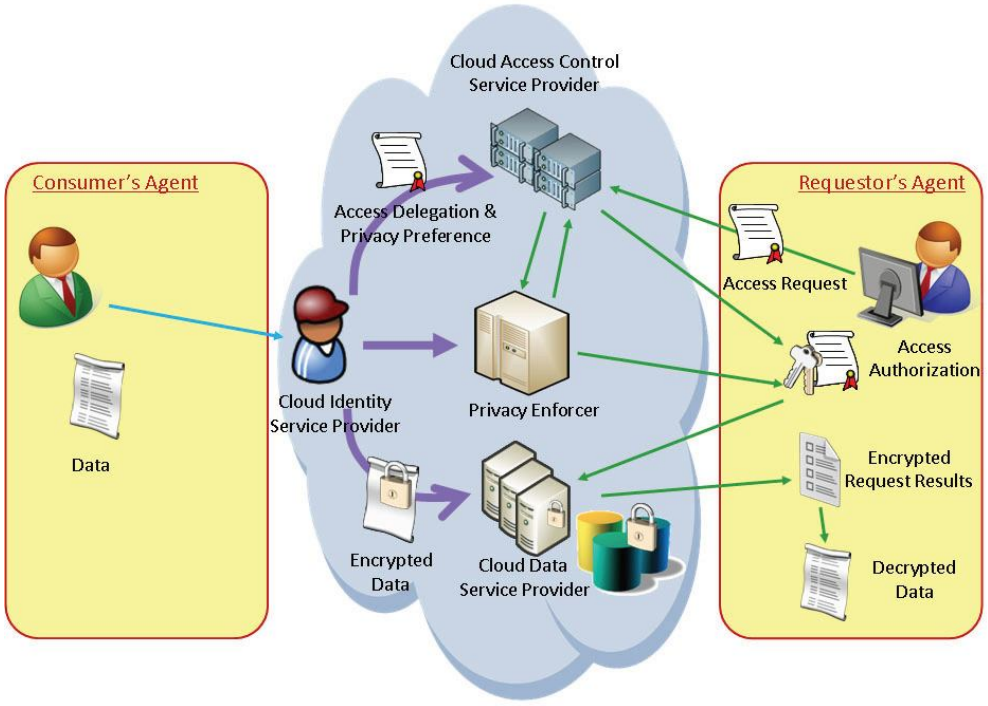
- Vérifiez si le fournisseur de nuage conserve des droits relatifs à vos données même lorsque vous les avez supprimées du nuage. Le cas échéant, demandez-vous si cela vous pose problème.
- Prévoyez des méthodes de protection des renseignements personnels dans votre modèle de mise en œuvre d'informatique en nuage.

5.2.2 Protection de la saisie de données dans le nuage

Un document sur l'utilisation des principes de Privacy by Design (PbD) en informatique en nuage fournit des suggestions en matière de méthode de protection des données envoyées vers le nuage et pour conserver un accès adéquat à ces données protégées (voir la Figure 8) (NEC et CIPVP Ontario, 2010) :

- Créer une architecture qui requiert la collaboration entre deux agents – l'agent du client et l'agent du demandeur – trois fournisseurs de services – le fournisseur de services de contrôle d'accès du nuage, le fournisseur de services de données du nuage et le fournisseur de services d'identification du nuage – et un responsable de la protection des renseignements personnels.
- L'agent du client sera chargé de chiffrer les données avant de les envoyer vers le nuage et de déléguer l'accès au fournisseur de services de contrôle d'accès du nuage qui traitera les demandes d'utilisation des données provenant du demandeur.
- En raison de l'architecture, l'agent du demandeur devra communiquer avec le fournisseur de services de contrôle d'accès du nuage pour obtenir une autorisation d'accès.
- Le fournisseur de services d'identification du nuage aidera le client à gérer les identités en protégeant les pseudonymes sûrs et gérables et en fournissant des pseudonymes aux clients.
- Le responsable de la protection des renseignements personnels fera correspondre les fins indiquées par le demandeur aux préférences du client en matière de protection des renseignements personnels.
- Le message d'autorisation comportera trois éléments : i) il indiquera au fournisseur de services de contrôle d'accès du nuage que le demandeur a été authentifié; ii) il indiquera le sous-ensemble de données à envoyer au demandeur; et iii) il contiendra également une clé de déchiffrement des données envoyées.

Figure 8 : Architecture de l'informatique en nuage pour assurer la protection des renseignements personnels et l'impartition de données utilisables



Source : *Modeling Cloud Computing Architecture without Compromising Privacy: A Privacy by Design Approach* (NEC et CIPVP Ontario, 2010)

5.2.3 Protection des données enregistrées par des tiers

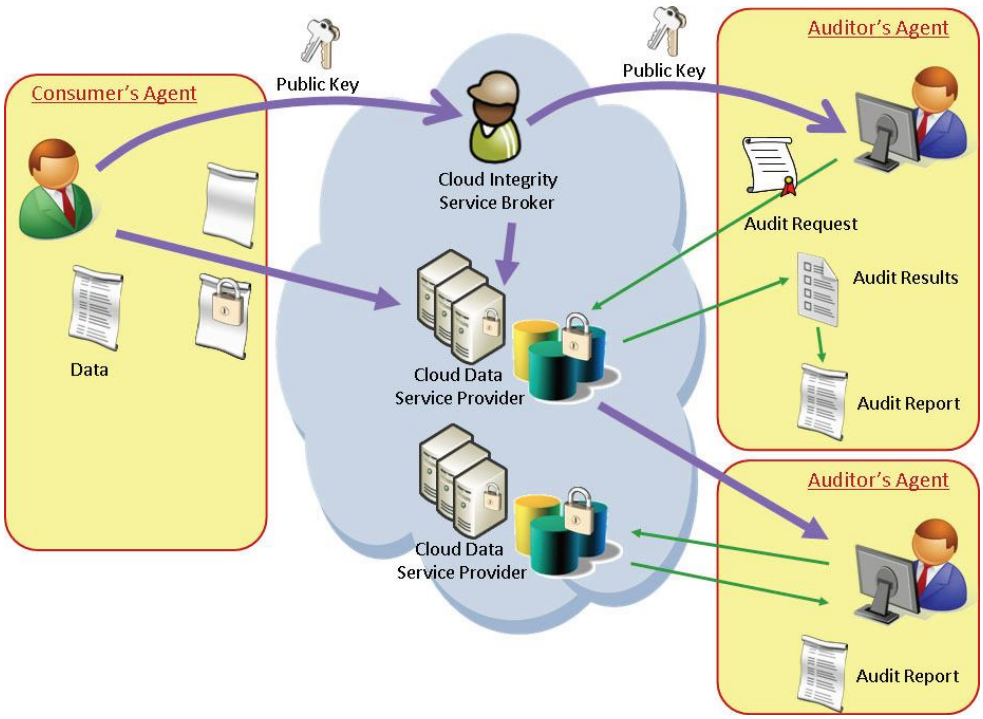
Quelques suggestions pour assurer l'intégrité des données protégées, sans atteinte à la confidentialité, lorsque le fournisseur de services de données dans le nuage utilise d'autres fournisseurs de services de données dans le nuage comme méthode de secours (voir la Figure 9) (NEC et CIPVP Ontario, 2010) :

- Créer une architecture qui requiert la collaboration entre deux types d'agents – l'agent du client et l'agent du vérificateur – un fournisseur de services de données (remanié) et un courtier de services d'intégrité dans le nuage.
- L'agent du client procède à l'impartition des données chiffrées vers le fournisseur de services de données dans le nuage, et maintenant on fait également affaire avec un vérificateur (interne ou externe au client) pour gérer les vérifications de l'intégrité.
- Le courtier de services d'intégrité dans le nuage aide le client et le fournisseur de services de données dans le nuage à embaucher des vérificateurs et à transmettre la clé publique du client aux vérificateurs et au fournisseur de services de données dans le nuage.
- Le vérificateur envoie les demandes de vérification au fournisseur de services de données dans le nuage, qui répond en envoyant le résultat de la vérification. Le vérificateur envoie ensuite un rapport de vérification sur l'intégrité des données.

- Il est essentiel dans cette architecture que le client utilise une clé publique plutôt qu'une clé de chiffrement, même si le fournisseur de services de données dans le nuage et l'agent du vérificateur sont compromis, les données du client et donc la confidentialité sont protégées.
- Pour un niveau accru de protection des renseignements personnels, on peut ajouter un fournisseur de services d'identification du nuage dans cette architecture de vérification afin de permettre au client de trouver un vérificateur de façon anonyme ou en utilisant un pseudonyme et en évitant qu'un vérificateur malveillant obtienne tout avantage en termes d'invasion de la confidentialité simplement en étant embauché pour vérifier les données d'un client.

Ces idées de conception de l'architecture visent à permettre le respect de façon simultanée des exigences en matière de sécurité, de capacité d'utilisation, d'intégrité des données et de protection des renseignements personnels; la « somme positive » que le respect des principes de PbD permet d'atteindre.

Figure 9 : Architecture de l'informatique en nuage pour la protection des renseignements personnels et l'impartition de données sûres et accessibles



Source : *Modeling Cloud Computing Architecture without Compromising Privacy: A Privacy by Design Approach* (NEC et CIPVP Ontario, 2010)

5.3 Questions juridiques/responsabilité

Les sections suivantes présentent les pratiques exemplaires suggérées pour gérer les contrats et les accords sur les niveaux de service avec les fournisseurs de services dans le nuage.

5.3.1 Contrats

Quelques raisons de conclure des contrats avec des fournisseurs d'informatique en nuage (McDonald, 2010), Badger, *et coll.* (2011) et (Corley, 2011) :

- *Protection des renseignements personnels et confidentialité*
  - Assurez-vous, par le biais de clauses de contrats précises, que le fournisseur n'utilisera pas les données à d'autres fins que pour fournir le service imparti (comme l'extraction de données à son propre avantage) ou qu'il ne les divulguera pas à autrui sans avoir obtenu l'autorisation nécessaire.
  - Analysez les méthodes de protection des données des SaaS et PaaS du fournisseur, la configuration de l'emplacement des données, l'organisation des bases de données et les technologies de traitement des opérations et déterminez s'ils satisfont à vos exigences en matière de confidentialité et de conformité.
- *Sécurité des données*
  - Indiquez une norme de sécurité réelle, précise et indépendante et demandez qu'elle soit mise à jour et peut-être vérifiée (p. ex. SAS 70, vérification de Type II) régulièrement et demandez au fournisseur de vous avertir de toute atteinte à la sécurité ou aux données.
  - Demandez au fournisseur de proposer un mécanisme permettant de supprimer des données de façon fiable et sûre à la demande d'un abonné.
  - Demandez aux fournisseurs de SaaS d'utiliser une solide méthode de chiffrement qui emploie un algorithme robuste et des clés suffisamment fortes pour les sessions Web dès que l'application fournie nécessite la confidentialité de l'interaction de l'application et des transferts de données. Demandez également que la même diligence s'applique aux données entreposées.
  - Veillez à ce qu'il soit possible de configurer une application PaaS afin qu'elle fonctionne de façon sûre et qu'on puisse l'intégrer dans les cadres de sécurité de l'entreprise qui existent déjà comme un processus d'identification et d'autorisation.
  - S'assurer que les fournisseurs d'IaaS ont établi des mécanismes pour protéger les machines virtuelles des attaques a) provenant d'autres MV qui se trouvent sur le même hôte physique b) provenant de l'hôte physique lui-même c) et provenant du réseau.
  - Demandez aux fournisseurs de proposer des méthodes que l'abonné peut utiliser pour évaluer si ses exigences en matière de protection des données continuent d'être satisfaites.
  - Pour le chiffrement des données stockées, demandez au fournisseur de rendre accessibles la robustesse de l'ensemble d'algorithmes de chiffrement, les principales méthodes de gestion des clés que le fournisseur prend en charge et le nombre de clés pour chaque propriétaire de données (clés personnelles ou partagées).

- *Emplacement des données*
  - Si vous y tenez, ajoutez une clause interdisant l'entreposage « extraterritorial » (p. ex. aux États-Unis).
- *Accès aux données*
  - Envisagez d'ajouter des conditions contractuelles relatives à la garantie et la mise à l'épreuve de l'intégrité des données, aux formats des données, à la fréquence des copies de secours, à l'entreposage des données copiées, à l'accès aux données si le fournisseur disparaît, aux défaillances, etc.
- *Responsabilité des utilisateurs finaux*
  - Afin de respecter les exigences normales du fournisseur qui requièrent que les utilisateurs finaux respectent la politique en matière d'utilisation acceptable, les conditions de service ou les dispositions similaires, demandez aux utilisateurs finaux de s'entendre directement avec le fournisseur en ce qui a trait au respect de ces dispositions.
- *Utilisation non autorisée ou inadéquate*
  - Indiquez uniquement que vous n'« autoriserez » pas ou que vous ne « permettrez pas en connaissance de cause » toute utilisation « non autorisée » ou « inadéquate » du service du fournisseur par d'autres personnes et que vous signalerez uniquement les utilisations « graves ».
- *Suspension des comptes d'utilisateurs finaux*
  - Autorisez la suspension des droits des utilisateurs finaux uniquement en cas d'infractions « graves » à la politique sur l'utilisation acceptable du fournisseur, aux conditions de services ou à des dispositions similaires ou en cas d'infractions qui menacent « gravement » la sécurité ou l'intégrité du système du fournisseur.
- *Questions de sécurité en cas d'urgence*
  - Il faut définir clairement la norme relative à ce qui constitue une interruption de l'utilisation en cas d'urgence. Elle doit donner au fournisseur peu ou pas du tout de latitude ou de souplesse dans son application; elle doit de préférence intégrer un seuil de « gravité » ou d'un élément similaire.
- *Interruption et cessation de service*
  - La portée des dispositions sur la cessation de services doit être limitée aux problèmes vraiment importants. Elle doit vous permettre de gérer les infractions présumées ou d'avoir recours à la hiérarchie au lieu de privilégier l'application instantanée (sauf en cas de véritables urgences). Elle doit vous donner suffisamment de temps pour prendre d'autres arrangements pour vos données ou votre service.
- *Propriété des données*
  - Le contrat doit clairement indiquer que l'ensemble des données appartient à votre organisation (et/ou à vos utilisateurs) et que le fournisseur n'acquiert aucun droit ou aucune licence pour l'utilisation des données à des fins personnelles en vertu de la transaction et qu'il n'acquiert pas non plus d'intérêt relatif à la sécurité des données et ne peut pas en faire la demande.

- *Accords sur les niveaux de service*
  - Énoncez clairement le « temps de disponibilité » garanti, le processus et la durée nécessaires pour gérer le « temps d'indisponibilité » et les conséquences en cas de non-respect de ces exigences.
  - Formulez des méthodes de recours adéquates en fonction des dommages qui peuvent survenir.
  - Précisez la conformité avec des lois et règlements donnés qui régissent les données de l'abonné.
  - Assurez-vous qu'il n'existe pas de clause de non-responsabilité relative à la sécurité ou au traitement critique.
  - Cherchez les recommandations du fournisseur sur la copie de secours indépendantes des données conservées dans son nuage.
- *Exonération de garantie*
  - Le contrat doit stipuler que le service est conforme au cahier de charges et qu'il fonctionnera comme prévu (le cahier de charges doit être aussi détaillé que possible pour éviter tout malentendu et désaccord) et qu'il n'enfreint pas les droits relatifs à la propriété intellectuelle de qui que ce soit.
- *Indemnisation par le fournisseur*
  - Le fournisseur doit vous indemniser pour ses actions ou ses omissions, particulièrement pour l'infraction aux droits relatifs à la propriété intellectuelle d'autrui et pour la divulgation inadéquate des données ou l'atteinte aux données.
- *Modifications du contrat*
  - Limitez les droits du fournisseur qui lui permettent de modifier son service aux modifications raisonnables sur le plan commercial, à condition que les modifications ne diminuent pas de façon importante la nature, la portée ou la qualité du service.
- *Incorporation de conditions générales sur les URL*
  - En ce qui a trait aux références incluses dans le contrat qui renvoient vers d'autres conditions générales et politiques affichées sur le site Web du fournisseur, essayez de demander au fournisseur de vous avertir directement suffisamment tôt avant la date d'entrée en vigueur de toute modification apportée aux modalités intégrées, et de vous permettre de mettre fin au service si les modifications sont inacceptables ou si elles nuisent gravement aux intérêts des clients.
- *Renouvellement automatique*
  - Idéalement, le contrat doit être renouvelé automatiquement (vous n'avez donc pas besoin de le renégocier chaque fois), mais il doit également permettre de mettre fin au service en fournissant un préavis raisonnablement court.
- *Cessation de service*
  - Assurez-vous que le contrat décrit les circonstances et les conditions générales en vertu desquelles une partie peut mettre fin à l'entente avant sa date d'expiration et les droits et responsabilités des parties dans chaque situation.
- *Loi applicable et compétence*
  - Il est préférable : (a) d'indiquer la loi et la compétence de votre province; (b) d'indiquer que les différends doivent être réglés dans la province du défendeur; ou (c) de supprimer la

disposition contractuelle normalisée du fournisseur et de laisser la question ouverte afin de la traiter plus tard s'il y a lieu.
    - Analysez des effets potentiels des exigences contractuelles, législatives ou réglementaires (p. ex. divulgation obligatoire de données, possible saisie de données, etc.), la capacité du fournisseur à s'adapter aux nouveaux règlements ou à d'autres changements obligatoires et la possibilité que le fournisseur déménage vers une autre province.
- *Transitions initiale et finale*
    - Les dispositions relatives à la transition initiale doivent indiquer la façon dont les données et les services seront transférés au fournisseur de façon ordonnée et efficace ainsi que le soutien adéquat du fournisseur.
    - Les dispositions relatives à la transition finale doivent prévoir un transfert ordonné et efficace vers le client ou un autre fournisseur, afin d'assurer la continuité du service et l'intégrité des données.

5.3.2 Accords sur les niveaux de service

Selon le Groupe de consultation sur l'informatique en nuage de l'ITU, les accords sur les niveaux de service (ANS) doivent porter sur les éléments suivants (Weissberger, 2011b) :

Point de vue des utilisateurs du service

Élément	Description
Responsabilités	Les utilisateurs du service dans le nuage doivent être responsables des limites d'utilisation du système et des restrictions relatives aux types de données qui peuvent être entreposées.
Poursuite des activités et rétablissement après une catastrophe	Les utilisateurs du service dans le nuage doivent s'assurer que leur fournisseur de nuage a établi des mécanismes de protection adéquats en cas de catastrophe.
Redondance des systèmes	Les utilisateurs du service dans le nuage qui déplacent des données et des applications qui doivent être accessibles en tout temps doivent analyser la redondance des systèmes de leurs fournisseurs.
Entretien	Les utilisateurs du service dans le nuage doivent savoir comment et quand leurs fournisseurs procéderont à l'entretien.
Emplacement des données	Les utilisateurs du service dans le nuage doivent pouvoir réaliser une vérification du fournisseur afin de s'assurer qu'il respecte les règlements si un fournisseur de services dans le nuage promet de respecter les règlements sur l'emplacement des données.
Sécurité	Les utilisateurs du service dans le nuage doivent connaître leurs besoins en matière de sécurité et les méthodes de contrôle et de fédération nécessaires pour satisfaire à ces besoins.
Transparence	Les utilisateurs du service dans le nuage sont chargés de prouver que leur fournisseur n'a pas respecté les conditions prévues l'ANS, en vertu des ANS de certains fournisseurs de nuage.

Élément	Description
Certification	Les utilisateurs du service dans le nuage pourraient être assujettis à des obligations en matière de certification et devoir s'assurer que leur fournisseur de nuage est certifié en vertu de la norme ISO 27001.

Point de vue des fournisseurs de services

Élément	Description
Sécurité	Le fournisseur doit savoir ce qu'il doit fournir aux utilisateurs du service afin de mettre en place des méthodes adéquates de contrôle et de fédération.
Chiffrement des données	L'ANS doit fournir des détails sur les algorithmes de chiffrement et sur les politiques de contrôle de l'accès.
Protection des renseignements personnels	L'ANS doit indiquer clairement la façon dont le fournisseur de nuage isole les données et les applications dans un environnement pluripartite.
Conservation et suppression des données	Le fournisseur de nuage doit pouvoir conserver les données pendant une certaine période et les supprimer après une certaine période.
Effacement et destruction du matériel	Le fournisseur de nuage doit offrir une protection ajoutée assurant l'effacement de l'espace mémoire lorsqu'un client éteint une MV.
Conformité réglementaire	Le fournisseur de nuage doit pouvoir prouver sa conformité si un règlement s'applique.
Transparence	Le fournisseur de nuage doit de façon proactive informer les clients en cas d'infraction aux conditions de l'ANS en ce qui a trait aux données et aux applications essentielles.
Certification	Le fournisseur de nuage sera tenu de prouver qu'il est certifié et de se tenir à jour.

Exigences communes

Élément	Description
Terminologie pour les principaux indicateurs de rendement	Un ensemble de termes définis par l'industrie pour différents indicateurs clés du rendement faciliterait grandement la comparaison des ANS en particulier (et des services dans le nuage en général).
Suivi	Il faut tenir compte de la question de confiance pendant l'exécution de l'ANS. Par exemple, les clients peuvent ne pas faire entièrement confiance à certaines mesures fournies uniquement par un fournisseur de services et avoir régulièrement recours à un organisme tiers neutre. Cet organisme est chargé de surveiller et de mesurer les paramètres de service essentiels et de signaler les infractions à l'entente commises par le client et par le fournisseur. Cette mesure peut permettre d'éliminer les conflits d'intérêts qui peuvent survenir si le fournisseur signale des interruptions de services à son entière discrétion ou si le client est chargé de prouver qu'une interruption a eu

Élément	Description
	lieu.
Possibilité de vérification	Il est essentiel que les utilisateurs du service vérifient les systèmes et les procédures du fournisseur. L'ANS doit donc indiquer clairement la façon dont les vérifications doivent avoir lieu ainsi que le moment où elles doivent se produire.
Mesures	Le suivi et la vérification requièrent un élément tangible qui peut être surveillé lorsqu'il se produit et vérifié par la suite. Les mesures de l'ANS doivent être définies de façon objective et non ambiguë.
ANS lisibles par machine	Des ANS lisibles par machine permettraient d'utiliser un courtier en nuage automatisé qui pourrait sélectionner un fournisseur de nuage de façon dynamique. L'une des caractéristiques de base de l'informatique en nuage est le libre service à la demande; un courtier en nuage automatisé permettrait d'élargir cette caractéristique en sélectionnant le fournisseur de nuage à la demande également. Le courtier pourrait sélectionner un fournisseur de nuage en fonction des critères opérationnels définis par le client.
Interaction humaine	Bien que le libre service à la demande soit une caractéristique de base de l'informatique en nuage, il n'en demeure pas moins qu'il y aura toujours des problèmes que seuls les êtres humains pourront régler. Ces situations doivent être rares, mais bon nombre d'ANS comporteront des garanties relatives à la réponse du fournisseur aux demandes de soutien.
Courtiers et revendeurs du nuage	Si un fournisseur de nuage est en fait un courtier ou un revendeur auprès d'un autre fournisseur de nuage, les conditions de l'ANS doivent indiquer clairement toute question de responsabilité si un problème survient dans les installations du courtier, du revendeur ou du fournisseur.

5.4 Règlements et normes

L'Open Data Centre Alliance (ODCA) a conçu les modèles d'utilisation sûre suivants pour l'informatique en nuage :

- *Open Data Center Alliance Usage : Virtual Machine (VM) Interoperability* (ODCA, 2011c) – indique les mesures et les processus qui favorisent la création de solutions de gestion de machine virtuelle interexploitables afin de diminuer la complexité et le prix de la gestion, particulièrement dans des environnements hétérogènes où l'on trouve plusieurs fournisseurs.
- *Open Données Center Alliance Usage : Regulatory Framework* (ODCA, 2011d) – aide les organisations utilisatrices à évaluer et surveiller leurs obligations réglementaires lorsqu'ils participent aux services dans le nuage ou en font l'acquisition.

5.5 Gestion du changement

Quelques difficultés en matière de gestion du changement que les dirigeants principaux de l'information (DPI) peuvent s'attendre à devoir surmonter pendant l'adoption de solutions d'informatique en nuage (Spires, 2011) :

- Les DPI doivent collaborer étroitement avec les communautés chargées de l'acquisition, de l'approvisionnement et des finances afin de gérer le nouveau paradigme opérationnel que représente l'informatique en nuage, car les principales questions relatives à la gestion du changement visent les modèles opérationnels et contractuels.
- Les DPI devront traiter les changements dans la main-d'œuvre; alors que le nuage transformera la prestation de services, ils devront fournir du leadership pour gérer la mise à jour des compétences du personnel existant ainsi que le recrutement de nouveaux membres.
- Les DPI doivent évaluer les compromis entre les avantages de l'informatique dans le nuage public et les risques en matière de sécurité liés à la gestion et à l'entreposage de données sensibles.
- Les DPI devront adapter les modèles de gouvernance et de gestion en fonction du profit que le reste de l'organisation des TI tire de l'informatique en nuage.

5.6 Fiabilité et rendement

L'Open Data Centre Alliance (ODCA) a conçu les modèles d'utilisation sûre suivants pour l'informatique en nuage :

- *Open Data Center Alliance Usage : Standard Units of Measure for IaaS* (ODCA, 2011e) – fournit aux abonnés de services dans le nuage un cadre et des attributs connexes utilisés pour décrire et mesurer la capacité, le rendement et la qualité d'un service dans le nuage.

Annexe 4 : Nuage géospatial *c.* SIG d'entreprise

Solution d'informatique en nuage géospatiale	Solution opérationnelle classique de SIG d'entreprise
Généralités	
Solution générale, propre à aucune organisation en particulier. Mise en œuvre rapide. Facile à apprendre et à utiliser. Solution éprouvée auprès de plusieurs clients et dans diverses configurations. En règle générale destinée à des utilisateurs non experts, mais donne accès aux données au personnel du SIG et fournit des applications bureautiques.	Solution conçue et créée en fonction des besoins de l'organisation. Il peut être difficile de concevoir la solution afin de permettre l'évolution et les modifications. Le processus de conception, de création et de mise en œuvre peut durer des mois voire des années. Les solutions internes ne sont pas éprouvées et présentent donc un risque élevé. Dépendance sur des ressources ministérielles ou des personnes embauchées pour l'entretien et la gestion.
Applications et outils	
Logiciel de base : le logiciel de base et les applications sont inclus. **Fonctionnalité pour l'utilisateur** : en règle générale, seuls les outils généraux qui offrent un accès de base aux cartes, l'intégration, la visualisation et un ensemble de base d'analyses spatiales. **Fonctionnalité pour la gestion** : la solution peut contenir d'autres fonctionnalités opérationnelles comme la gestion de documents, la déclaration de bases de données opérationnelles. Fonctionne dans le navigateur donc presque toujours accessible (sauf en cas d'interruption programmée ou d'urgence). Fonctionnalité pour la gestion des comptes, la configuration, la sécurité, intégrée.	**Logiciel de base** : il faut obtenir les licences pour les logiciels de gestion de bases de données, le SIG, le système d'exploitation, les services Web, etc. **Fonctionnalité pour l'utilisateur** : applications personnalisées conçues ou adaptées pour satisfaire aux besoins. **Fonctionnalité pour la gestion** : besoin de gérer la mise à jour du logiciel, les différentes versions et les mises à niveau au gré de leur publication – souvent de fournisseurs multiples. Il faut personnaliser la solution pour satisfaire aux besoins particuliers. Il faut prévoir une capacité de gestion/entretien pour la gestion des comptes d'utilisateur, la sécurité, etc.
Infrastructure informatique	
L'infrastructure informatique est comprise. Rendement du système garanti et amples ressources informatiques fournies pour répondre aux besoins et termes d'évolution et de forte utilisation. Il est possible de gérer immédiatement les changements des besoins en termes d'utilisation.	Infrastructure informatique achetée ou louée, configurée et gérée par des ressources internes dédiées. Le rendement et la capacité du système ne sont en règle générale pas configurés pour une forte utilisation, pour les pics ou les changements liés à la demande de service. Il est difficile de prendre en charge les changements des besoins en termes d'utilisation et de ressources.

Solution d'informatique en nuage géospatiale	Solution opérationnelle classique de SIG d'entreprise
Contenu	
Inclut presque toujours des données de base spatiales. Inclut ou intègre souvent les services d'information Web d'un tiers pour une valeur ajoutée.	En règle générale, il incombe à l'organisation de gérer et de mettre à jour les données, une mesure qui peut nécessiter des efforts et des coûts. On peut compléter les données de l'organisation avec un service de DaaS. Les données spatiales requièrent un logiciel et du personnel spécialisés. Peut nécessiter des négociations avec les propriétaires des données pour accéder au contenu.
Sécurité	
Solides mécanismes de sécurité en place, ou le fournisseur pourrait perdre son entreprise. La sécurité est en règle générale vérifiée et documentée, bien qu'il soit difficile pour les utilisateurs d'accéder à ces renseignements. Dans certaines configurations, l'« architecture répartie » permet de protéger les données par le pare-feu du client.	La sécurité doit être intégrée à l'application, notamment la gestion des comptes d'utilisateurs et l'accès fondé sur des règles. La sécurité est essentielle à la réussite du système, spécialement si le système accède aux données dans des domaines qui ont des niveaux et des degrés d'accès variables. Capacités hautement spécialisées requises.
Poursuite des activités	
La plupart des fournisseurs d'informatique en nuage disposent de plusieurs éléments pour assurer la poursuite des activités : • Redondance de l'infrastructure informatique pour une accessibilité élevée et aucune défaillance. • Sauvegarde continue des données et du logiciel. • Ententes sur l'entretien pour les organisations indiquant les fournisseurs de logiciels et de matériel. • Suivi et mise à l'épreuve continus des systèmes.	Il faut concevoir un plan de poursuite des activités et le mettre en œuvre pour assurer l'accessibilité adéquate à l'ensemble des composantes du système (applications, infrastructure et données). Il faut des professionnels dédiés pour fournir et gérer la solution. Il peut revenir cher d'alimenter une solution à forte accessibilité. La création et l'entretien coûtent cher.
Soutien à la clientèle	
En règle générale, processus de gestion des incidents clair. Des accords sur les niveaux de service (ANS) doivent exister. Il peut être difficile d'assurer des voies de communication claires avec un seul point de contact. Cependant un fournisseur gère tous les problèmes.	Il faut définir, établir et exécuter des procédures internes de soutien à la clientèle et des indicateurs clés du rendement. Il y a souvent plusieurs fournisseurs et donc aucun point unique de responsabilité. Le service à la clientèle pose souvent problème. Le soutien à la clientèle et la gestion des relations manquent souvent de clarté.

Solution d'informatique en nuage géospatiale	Solution opérationnelle classique de SIG d'entreprise
Coûts	
Souvent un modèle d'abonnement. Prévisible. En règle générale abordable ou peut être conçu de façon abordable en fonction des besoins.	Coûts inconnus et imprévisibles au début et continus. De multiples fournisseurs et de multiples factures peuvent entraîner des erreurs, des écarts, des coûts et une administration accrus.