Document de travail/Working Paper

Laboratoire de CYBERJUSTICE Laboratory

N° : 11

Titre/Title : ÉTUDE SUR LES INCIDENCES JURIDIQUES DE L'UTILISATION DE L'INFONUAGIQUE PAR LE GOUVERNEMENT DU QUÉBEC

Date : 10 juillet 2014

Auteur(s)/Author(s) : Me Nicolas VERMEYS, Me Julie M. GAUTHIER et Me Sarit MIZRAHI

Courriel/Email : nicolas.vermeys@umontreal.ca

Résumé/Abstract (300-500 mots/words) :

L'infonuagique présente cinq grandes caractéristiques (le libre-service sur demande,l'accès global au réseau, un bassin de ressources, la souplesse rapide et les services mesurés) et peut être envisagé selon différents modèles de déploiement (privé interne, privé externe, public, communautaire et hybride) et de service (logiciels sous forme de service, plateforme sous forme de service, infrastructure sous forme de service, etc.) possédant chacun leurs avantages et leurs inconvénients. Toutefois, si la technologie elle-même n'est pas proscrite, certains des modèles d'affaires proposés par les prestataires de services infonuagiques ne concordent pas avec les obligations imposées aux organismes publics quant à la protection de l'intégrité, de la disponibilité et de la confidentialité des informations personnelles et autrement confidentielles qu'ils détiennent. En effet, les risques associés au recours à l'infonuagique seront d'abord et avant tout fonction du type de données contenues dans ou accessibles via les documents technologiques hébergés dans le nuage ou circulant par le biais de celui-ci. Or, tant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels que la Loi concernant le cadre juridique des technologies de l'information viennent baliser les possibilités offertes par l'infonuagique, notamment en interdisant d'héberger des renseignements personnels ou autrement confidentiels dans un nuage dont les serveurs résideraient à l'extérieur du Québec ou seraient sous le contrôle d'une entreprise étrangère. La Loi sur l'accès permet toutefois de passer outre cette interdiction lorsque les lois applicables au territoire hôte offrent une protection équivalente au cadre juridique québécois. Cette exception permettrait donc, vu l'équivalence présumée des lois en vigueur sur ces territoires, d'héberger des renseignements confidentiels dans un nuage canadien, voire même possiblement européen. Toutefois, l'hébergement de données confidentielles dans un nuage états-unien soulève de nombreuses controverses vu les droits accordés aux autorités américaines par le USA PATRIOT Act et, de ce fait, ne semble pas possible à la lumière des textes de loi précités. Ceci étant, même s'il semble impossible de concilier la lettre de la Loi sur l'accès et le recours à un nuage international, l'esprit de la loi serait protégé si les organismes publics procédaient au chiffrement des données avant de les verser dans le nuage ou de les faire circuler par le biais de celui-ci. Si cette solution ne résiste pas à une analyse textuelle de la Loi sur l'accès, elle s'avère toutefois plus réaliste vu la mondialisation des marchés et, surtout, les engagements pris par le Québec envers ses partenaires commerciaux internationaux.

ÉTUDE SUR LES INCIDENCES JURIDIQUES DE L'UTILISATION DE L'INFONUAGIQUE PAR LE GOUVERNEMENT DU QUÉBEC

Par

Me Nicolas VERMEYS
Me Julie M. GAUTHIER
Me Sarit MIZRAHI

La présente étude a été financée par le Secrétariat du Conseil du trésor et produite par M^e^ Nicolas Vermeys, professeur à la Faculté de droit de l'Université de Montréal, directeur adjoint du Laboratoire de cyberjustice et chercheur au Centre de recherche en droit public avec la collaboration de M^es^ Julie M. Gauthier et Sarit Mizrahi. À cet égard, il importe de souligner que les positions qui y sont défendues constituent celles des seuls auteurs.

Les auteurs aimeraient par ailleurs remercier les membres du comité consultatif *ad hoc* issu du gouvernement du Québec pour leurs commentaires, critiques et conseils. Un merci particulier est adressé à messieurs Patrick Gingras, Dave Tanguy et Dieu Hang pour leurs nombreux retours et éclaircissements.

TABLE DES MATIÈRES

RÉSUMÉ

Selon le NIST, l'infonuagique (ou informatique en nuage) est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le prestataire de services. L'infonuagique présente cinq grandes caractéristiques (le libre-service sur demande, l'accès global au réseau, un bassin de ressources, la souplesse rapide et les services mesurés) et peut être envisagé selon différents modèles de déploiement (privé interne, privé externe, public, communautaire et hybride) et de service (logiciels sous forme de service, plateforme sous forme de service, infrastructure sous forme de service, etc.) possédant chacun leurs avantages et leurs inconvénients. Du point de vue juridique, le fait, pour un organisme ou ministère de déposer ou faire circuler des renseignements dans le nuage, même s'ils sont confidentiels, n'est interdit par aucun texte de loi. D'ailleurs, plusieurs juridictions ailleurs au Canada et à travers le monde ont choisi de profiter des avantages offerts par l'informatique en nuage. Toutefois, si la technologie elle-même n'est pas proscrite, certains des modèles d'affaires proposés par les prestataires de services infonuagiques ne concordent pas avec les obligations imposées aux organismes publics quant à la protection de l'intégrité, de la disponibilité et de la confidentialité des informations personnelles et autrement confidentielles qu'ils détiennent.

En effet, les risques associés au recours à l'infonuagique seront d'abord et avant tout fonction du type de données contenues dans ou accessibles via les documents technologiques hébergés dans le nuage ou circulant par le biais de celui-ci. Ainsi, si tous les documents hébergés ont un caractère public, la mise en place de mesures de sécurité visant à en empêcher l'interception ou la consultation par un tiers deviendra moins pertinente. Ce ne sera donc que lorsqu'un renseignement se doit d'être protégé en vertu d'un texte de loi ou d'obligations contractuelles que son hébergement dans le nuage deviendra source de soucis.

Or, tant la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* que la *Loi concernant le cadre juridique des technologies de l'information* viennent baliser les possibilités offertes par l'infonuagique, notamment en interdisant d'héberger des renseignements personnels ou autrement confidentiels dans un nuage dont les serveurs résideraient à l'extérieur du Québec ou seraient sous le contrôle d'une entreprise étrangère. La *Loi sur l'accès* permet toutefois de passer outre cette interdiction lorsque les lois applicables au territoire hôte offrent une protection équivalente au cadre juridique québécois. Cette exception permettrait donc, vu l'équivalence présumée des lois en vigueur sur ces territoires, d'héberger des renseignements confidentiels dans un nuage canadien, voire même possiblement européen. Toutefois, l'hébergement de données confidentielles dans un nuage états-unien soulève de nombreuses controverses vu les droits accordés aux autorités américaines par le *USA PATRIOT Act* et, de ce fait, ne semble pas possible à la lumière des textes de loi précités. Ceci étant, même s'il semble impossible de concilier la lettre de la *Loi sur l'accès* et le recours à un nuage international, l'esprit de la loi serait protégé si les organismes publics procédaient au chiffrement des données avant de les verser dans le nuage ou de les faire circuler par le biais de celui-ci. Si cette solution ne résiste pas à une analyse textuelle de la *Loi sur l'accès*, elle s'avère toutefois plus réaliste vu la mondialisation des marchés et, surtout, les engagements pris par le Québec envers ses partenaires commerciaux internationaux.

INTRODUCTION

La dématérialisation de l'information liée au passage d'un support physique – le papier – vers un support numérique ou, pour reprendre l'expression consacrée par le législateur québécois, « faisant appel aux technologies de l'information »[1], si elle est venue faciliter le traitement et la recherche de données, a également entraîné certaines complications quant à la sécurité de celles-ci. En effet, s'il suffisait de déposer le document papier dans un tiroir verrouillé pour en assurer la confidentialité (ou tout au moins un niveau de confidentialité raisonnable), l'équivalent technologique du verrou demeure difficile à décrire puisqu'il incorpore différentes technologies distinctes et relativement complexes à définir. Si le mécanisme d'une serrure demeure conceptuellement accessible, le fonctionnement des algorithmes de chiffrement associés à la protection de documents technologiques est quant à lui difficilement apprivoisable pour un néophyte. La complexité relative des mesures de sécurité à mettre en place pour protéger les données numériques est par ailleurs accentuée par la possibilité d'accéder à celles-ci par le biais d'Internet ou de réseaux privés. En effet, si l'accès à une information contenue sur un support physique nécessite un déplacement vers le lieu où ce support est situé, la même information contenue sur un support numérique peut être accessible de plusieurs lieux. Ceci implique donc qu'il n'est plus simplement nécessaire de sécuriser un lieu, mais un accès, ce qui s'avère beaucoup plus complexe.

Pourtant, malgré cette augmentation dans la complexité des mesures de sécurité à mettre en place pour assurer un niveau de sécurité adéquat aux données hébergées sur des supports technologiques, l'obligation imposée aux entités qui collectent, gèrent et hébergent ces données demeure la même : assurer un niveau de sécurité raisonnable aux données confidentielles contenues dans ces documents. Or, au lendemain des découvertes à l'effet que certains ressortissants chinois auraient piraté les serveurs d'organismes gouvernementaux canadiens[2], ou encore des accusations d'espionnage à l'égard du gouvernement américain suite aux révélations

[1] *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c. C-1.1, art. 3.

[2] Voir, par exemple, Greg WESTON, « Foreign hackers attack Canadian government », (2013) *CBC.ca*, en ligne : < http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618 >.

d'Edward Snowden, établir la « raisonnabilité » des mesures de sécurité mises en place pour protéger de telles données ouvre la porte à de nombreuses interrogations : où doit-on héberger ces données, qui doit être propriétaire des supports utilisés et, surtout, quelles données doivent être protégées.

La présente étude s'inscrit dans l'analyse de cette problématique en tentant de fournir des pistes de solution à ces questions, notamment en ce qui concerne l'hébergement délocalisé de données numériques, un phénomène aujourd'hui couramment – et parfois erronément – qualifié d'informatique en nuage ou d'infonuagique. En effet, la délocalisation, dans le nuage, des données (ou, tout au moins, des applications qui permettront de les traiter) soulève un certain nombre de questions juridiques liées à la sécurité de ces données, surtout lorsque celles-ci pourront être qualifiées de renseignements confidentiels. Si ces questions juridiques intéressent toute entité, elles sont particulièrement préoccupantes pour les gouvernements qui, plus souvent qu'autrement, font l'objet d'obligations plus importantes en ce qui concerne la sécurité des données qui leurs sont confiées. Ces obligations, si elles découlent souvent des attentes énoncées par la population en général, viennent également du législateur qui impose, comme nous le verrons, des normes de sécurité plus restrictives aux ministères et organismes gouvernementaux qu'aux entreprises privées. Ainsi, les risques juridiques associés à une éventuelle infonuagique gouvernementale québécoise sont, à bien des égards, plus importants que ceux auxquels serait confrontée une entreprise privée.

Bien que la définition de l'infonuagique fera l'objet d'une analyse particulière dans la présente étude, soulevons d'emblée que, en informatique :

> « le nuage (*cloud* en anglais) est l'image généralement utilisée pour symboliser graphiquement Internet. L'infonuagique, c'est en fait l'informatique vue comme un service et externalisée par l'intermédiaire d'Internet. Elle fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et reliés par Internet. Les ressources

> informatiques mises en commun et rendues ainsi disponibles à distance peuvent être, entre autres, des logiciels, de l'espace de stockage et des serveurs. »[3]

Ainsi, si l'image du nuage informatique est symboliquement assimilable au phénomène atmosphérique duquel il tire son nom, il ne faudrait pas en tirer de fausses conclusions. Comme l'a souligné le juge Mahoney dans l'affaire *Apple Computer*[4], « [l]a difficulté principale que j'ai rencontrée en l'espèce procède du caractère anthropomorphique de presque tout ce qui est pensé, dit ou écrit au sujet des ordinateurs. […] Les métaphores et analogies que nous utilisons pour décrire leurs différentes fonctions ne demeurent que des métaphores et des analogies »[5]. Ainsi, le nuage informatique, contrairement à son homonyme météorologique, n'erre pas ça et là au gré des changements atmosphériques. Si l'information qui y réside est effectivement dématérialisée et facilement transférable, elle demeure hébergée sur des serveurs qui, eux, sont bien ancrés à l'intérieur de locaux sous une juridiction bien précise. C'est donc dire qu'il est faux de prétendre que l'information contenue dans le nuage est partout et nulle part à la fois. Elle est en tout temps située à un endroit bien défini, même si cet endroit est inconnu de son détenteur juridique et bien qu'il puisse changer rapidement et régulièrement.

La présente étude vise donc, d'une part, à démystifier la notion d'infonuagique pour en tirer les avantages et inconvénients pour l'État québécois et, d'autre part, à identifier les contraintes juridiques et pratiques associées au recours, par le gouvernement du Québec, à ce type de service. Pour ce faire, la première section de l'étude effectuera une analyse détaillée de l'infonuagique ainsi que de ses différentes incarnations, de ses différents modèles. Elle fera également un survol d'un certain nombre d'initiatives étatiques d'ici et d'ailleurs qui ont fait recours à l'informatique en nuage afin d'en identifier les principaux obstacles et les balises à mettre en place pour assurer que le nuage ne vienne pas porter atteinte aux droits des citoyens ou sur-complexifier les obligations des ministères ou organismes. La deuxième section de l'étude viendra compléter

---

[3] OFFICE DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique,* en ligne : < http://www.granddictionnaire.com > (ci-après : l'« OLF »).

[4] *Apple Computer, Inc.* c. *Mackintosh Computers Ltd.*, (1987) 18 C.P.R. (3d) 129.

[5] *Id.*, par. 38.

l'analyse par un examen du cadre législatif applicable à l'infonuagique gouvernementale québécoise de façon générale et à certains scénarios plus précis.

Nous nous devons de préciser que la présente étude répond à une requête précise de la part du Secrétariat du Conseil du trésor afin d'étudier le cadre juridique relatif à la sécurité des informations hébergées ou traitées dans le nuage par un ministère ou organisme du gouvernement du Québec. Il serait donc erroné de tenter d'en étendre la portée au-delà de ce cadre analytique bien défini. Par ailleurs, il importe également de souligner que le contenu de l'étude vise à identifier les enseignements jurisprudentiels et doctrinaux liés à la question soumise. De ce fait, elle ne constitue pas un avis juridique et ne devrait aucunement être interprétée ainsi.

SECTION I : État des lieux relatifs à l'infonuagique

Tel que nous l'avons souligné en introduction, la présente étude se veut une analyse des risques juridiques[6] associés à l'utilisation de services infonuagiques par l'appareil étatique québécois. Or, une telle analyse repose sur l'acception d'une conception unique et bien définie des fondements, modèles et caractéristiques de l'infonuagique, afin d'assurer une compréhension partagée de cette notion souvent mal comprise (A). Ladite analyse repose également sur une compréhension des utilisations possibles de l'infonuagique par l'État québécois, utilisations qui peuvent être identifiées par un examen des recours à l'infonuagique par le gouvernement d'autres états, tant à l'intérieur qu'à l'extérieur des frontières canadiennes (B).

A. L'infonuagique : Description et modèles

Nous venons d'y faire allusion, l'infonuagique est une notion vaste et en constante évolution pour laquelle plusieurs définitions – lesquelles ne sont pas nécessairement équivalentes – ont été proposées. Malheureusement, comme aucune de ces définitions ne découle de la législation – le législateur (tout comme les tribunaux) ayant, à ce jour, choisi de rester muet quant à la portée de cette notion – c'est vers les divers écrits scientifiques que nous devons nous retourner. Ainsi, vu la disparité des opinions sur ce que constitue l'infonuagique, il nous faut, avant toute chose, effectuer un exercice sémantique afin de dégager les principaux éléments communs aux différentes définitions identifiées et, ainsi, de concevoir une définition de travail sur laquelle baser la présente étude.

L'Office québécois de la langue française définit l'infonuagique comme un : « [m]odèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation »[7].

[6] Par « risques juridiques », nous renvoyons aux risques de poursuite liés au non-respect d'une obligation législative.

[7] OLF, préc., note 3.

De son côté, le *National Institute of Standards and Technology* (« NIST ») états-unien fournit une définition plus précise selon laquelle :

> « L'infonuagique est un modèle d'accès au réseau habilitant, pratique et sur demande comprenant un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peut rapidement être activé et désactivé en réduisant au minimum les efforts de gestion ou les contacts avec le fournisseur de services. Ce modèle, qui favorise l'accessibilité, est composé de cinq caractéristiques essentielles, de trois modèles de service et de quatre modèles de mise en œuvre ».[8]

À la lumière de ces définitions, nous pouvons donc convenir que l'informatique en nuage ou « infonuagique » (terme qui sera repris dans la présente étude) est une expression générale définissant une nouvelle sorte d'infrastructure. Au lieu de développer les ressources informatiques à l'interne d'une organisation, il y a consommation des ressources par un « système qui stocke de l'information et/ou des applications en ligne, de manière à permettre à l'utilisateur d'y accéder à partir de n'importe quel dispositif »[9]. Dans un tel contexte, le système est opéré par « une interconnexion et une coopération de ressources informatiques, situées au sein d'une même entité ou dans diverses structures internes, externes ou mixtes, et dont les modes d'accès sont basés sur les protocoles et standards Internet »[10].

En d'autres mots, l'infonuagique repose sur « l'exploitation d'Internet et des notions de virtualisation pour créer un environnement dans lequel les personnes et les organisations peuvent acquérir de la capacité de stockage et de traitement »[11]. Il semble d'ailleurs qu'elle soit un

---

[8] Peter MELL et Timothy GRANCE, « The NIST Definition of Cloud Computing », version 15, en ligne : < http://csrc.nist.gov/ groups/SNS/cloud-computing/ > [Traduction du CPVPC].

[9] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA (ci-après : « CPVPC »), « Visez les nuages : Questions liées à la protection de la vie privée dans le contexte de l'informatique dans les nuages », (2010), en ligne : < http://www.priv.gc.ca/information/research-recherche/2010/cc_201003_f.asp#ftnref6 >.

[10] SYNTEC NUMÉRIQUE, « Livre blanc de la sécurité du Cloud Computing, Analyse des risques, réponses et bonnes pratiques », (2010), en ligne : <http://www.syntec-numerique.fr/sites/default/files/related_docs/livre_blanc_cloud_ computing_securite.vdef_.pdf >, p.6.

[11] INSITITUT CANADIEN DES COMPTABLES AGRÉÉS, « Infonuagique : Les grandes tendances technologiques », (2012), en ligne : < http://www.icca.ca/champs-dexpertise/gestion-de-linformation-et-technologies-de-linformation/les-grandes-tendances-technologiques/item72208.pdf >, p. 2.

concept de « déportation sur des serveurs distants des traitements informatiques traditionnellement effectués sur des serveurs locaux[12] ». Ainsi :

> « Les utilisateurs ou les entreprises ne sont plus gérants de leurs propres capacités informatiques, mais peuvent ainsi accéder de manière évolutive à de nombreux services en ligne sans avoir à gérer l'infrastructure sous-jacente, souvent complexe. Les applications et les données ne se trouvent plus sur l'ordinateur local, mais – métaphoriquement parlant – dans un « nuage » de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système ».[13]

L'infonuagique présente cinq grandes caractéristiques, soit le libre-service sur demande, l'accès global au réseau, un bassin de ressources, la souplesse rapide et les services mesurés[14]. En principe, ces attributs permettent une réduction des coûts et une augmentation de l'efficience et de l'efficacité organisationnelle[15]. En effet, l'infonuagique, lorsqu'utilisée de façon optimale, permettrait une utilisation plus efficiente des ressources informatiques[16], ainsi qu'une nette augmentation de l'efficacité des activités d'une organisation, notamment en facilitant la collaboration[17] entre employés et partenaires.

De plus, le libre-service sur demande avantagerait le recours à une telle technologie, puisque les dossiers d'une organisation seraient théoriquement accessibles n'importe où à partir d'une connexion réseau ou d'Internet. Ainsi, l'accès aux données se trouverait grandement facilité et il en résulterait une plus grande productivité pour le client. Qui plus est, l'hébergement des données dans le nuage pourrait aider à réduire les risques associés à la perte ou au vol de supports

---

[12] Patrick JOSET, « Cloud Computing, tentative de définition », (2011) *Abissa Informatique*, en ligne : < http://www.abissa.ch/data/fichiers/tec_cloud_computing.pdf >.

[13] *Id.*

[14] CPVPC, « Introduction à l'infonuagique », en ligne : < http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_f.pdf >.

[15] Mathieu TREMBLAY, « Services d'infonuagique (Synthèse de veille) », (2012) *Laboratoire d'étude sur les politiques publiques et la mondialisation (LEPPM)*, École nationale d'administration publique, p. 3.

[16] *Id.,* p. 4.

[17] Ann CAVOUKIAN, « Privacy in the clouds », (2008), en ligne : < http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf >.

matériels (clés USB, disques durs externes, etc.) autrefois nécessaires pour permettre le partage de données[18].

Les prestataires de services infonuagiques possèdent généralement l'échelle et l'infrastructure nécessaire pour permettre le partage efficace des ressources informatiques, comme l'interconnexion de réseaux et les centres de conservation de données. Ceci réduit le nombre de serveurs requis, en plus de limiter l'énergie, le refroidissement et l'espace nécessaire pour entreposer les serveurs. Le partage intelligent et organisé des données dans le nuage engendrerait ainsi une utilisation plus efficiente des ressources et une diminution de la quantité requise de celles-ci comparativement aux systèmes traditionnels[19]. De ce fait, les coûts associés à l'utilisation de l'infonuagique seraient, dans bien des cas, moindres que pour un système traditionnel[20].

Qui plus est, comme l'infonuagique ne requiert pas de l'utilisateur final qu'il procède à l'achat, l'installation et la mise en service de nouveaux effectifs informatiques afin de pouvoir avoir accès à de nouvelles applications, un tel modèle offrirait également un certain avantage au niveau de la rapidité de déploiement de nouvelles solutions logicielles. En effet, le cycle de déploiement des services s'en trouve grandement simplifié[21] et les utilisateurs peuvent donc se concentrer sur la mise en œuvre de services destinés à résoudre les problèmes de leur organisation, plutôt que d'investir dans le déploiement et la maintenance des infrastructures informatiques internes[22]. Le bassin de ressources et la souplesse rapide dont dispose le prestataire sont ainsi des atouts fort utiles pour les organisations.

---

[18] Lee BADGER, Tim GRANCE, Robert PATT-CORNER et Jeff VOAS, « Cloud computing synopsis and recommendations », (2012) *NIST*, en ligne : < http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075 >, p. 5-4.

[19] Eric BAUER et Randee ADAMS, *Reliability and Availability of Cloud Computing*, 1re éd., Hoboken, John Wiley & Sons, Inc., 2012, p. 15.

[20] Pour une étude sur l'économie de l'infonuagique, voir Jonathan LIEBENAU, Patrik KARRBERG, Alexander GROUS et Daniel CASTRO, « Modelling the Cloud », (2012) *LSE*, en ligne : < http://www.lse.ac.uk/businessAndConsultancy/LSEEnterprise/news/2012/cloud.pdf >.

[21] E. BAUER, préc., note 19, p. 14.

[22] *Id.*

Notons par ailleurs que l'extensibilité[23] et la souplesse de l'infonuagique permettent aux organisations d'effectuer une consommation ajustable des services en nuage. La puissance et la quantité d'espace requis seront en effet mesurées selon les besoins de l'organisation et les services fournis.

Évidemment, si l'infonuagique présente plusieurs avantages pour les organisations, elle comporte également certains risques et inconvénients associés, notamment, à la sécurité des données hébergées « dans le nuage » ou accessibles par le biais de celui-ci. Ces risques – lesquels pourront être généraux à tous les types d'infonuagique ou, tel que nous le verrons, particuliers à certains modèles de déploiement et de services – incluent notamment la perte ou la corruption de données lors de leur conservation, leur transmission, ou leur utilisation, ainsi que l'accès aux données par des tiers[24]. Évidemment, ces risques, s'ils sont bien réels, doivent toutefois être contextualisés. En effet, comme l'a soulevé le Commissariat à la protection de la vie privée du Canada :

> « Même si certains étaient d'avis que l'infonuagique pose certains risques pour la sécurité, d'autres considéraient qu'elle peut la renforcer si les fournisseurs sont en mesure d'utiliser des technologies et des méthodes de protection qui ne seraient pas habituellement mises en œuvre par des entreprises dans leurs propres centres de données ».[25]

Ainsi, les risques associés à l'infonuagique ne seront pas nécessairement plus importants que ceux qui découlent de l'hébergement de données à l'intérieur d'une organisation, si celle-ci ne bénéficie pas des moyens ou de l'expertise utile pour assurer un niveau de sécurité raisonnable aux données qu'elle détient.

---

[23] S. SUBASHINI et V. KAVITHA, « A survey on security issues in service delivery models of cloud computing », (2011) 34 *Journal of Network and Computer Applications* 1, 3.

[24] Ceci étant, ces risques sont les mêmes que ceux qui ont toujours guetté l'information. Voir Peter S. BROWNE, « Computer Security – A Survey », (1972) 4(3) *Database* 1.

[25] CPVPC, « Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique », (2011), en ligne : < http://www.priv.gc.ca/resource/consultations/report_201105_f.pdf >, p. 47.

Tout ce qui précède présente en quelque sorte l'infonuagique comme un concept monolithique, ce qui s'avère être une vision erronée de cette notion. En effet, le concept d'infonuagique vient englober différents modèles de déploiement (1) et de service (2) opérant dans le nuage et possédant leurs propres caractéristiques, avantages et inconvénients.

1) Les modèles de déploiement

Un modèle de déploiement fait référence à la manière selon laquelle est mis en œuvre un nouveau système informatique[26]. Selon une majorité d'auteurs, il existe quatre principaux modèles de déploiement dans le nuage, à savoir : le modèle public, le modèle privé, le modèle communautaire et le modèle hybride. Il importe donc, toujours afin de bien cerner ce que nous entendons par « infonuagique », d'identifier les spécificités propres à chaque modèle, ainsi que les principaux avantages et inconvénients découlant de leur utilisation.

Mentionnons d'emblée que, comme nous le verrons plus loin, le choix du modèle de déploiement aura des répercussions tant au niveau du droit à la vie privée que de la sécurité de l'information[27]. Toutefois, le niveau de sécurité dépendra en grande partie des mesures mises en place par l'organisation, de l'entente intervenue entre celle-ci et le prestataire et de la capacité de gérer l'environnement infonuagique. Comme le mentionne le NIST :

> [TRADUCTION] « [...] le modèle de déploiement en soi n'impose pas un niveau spécifique de sécurité ou de confidentialité. Ce niveau dépend plutôt des assurances, comme la sensibilité des politiques de sécurité et de confidentialité, la robustesse des contrôles de sécurité et de confidentialité, et l'étendue de la visibilité dans la performance et les détails de gestion de l'environnement infonuagique, qui peuvent tous être fournis par le fournisseur du nuage ou obtenus par l'organisation de manière indépendante (ex. : via les tests de vulnérabilité indépendants ou la vérification des opérations) ».[28]

---

[26] Voir OLF, préc., note 3.

[27] Voir Wayne JANSEN et Timothy GRANCE, « Guidelines on Security and Privacy in Public Cloud Computing », (2011) NIST, en ligne : < http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf >, p. 4.

[28] *Id.*

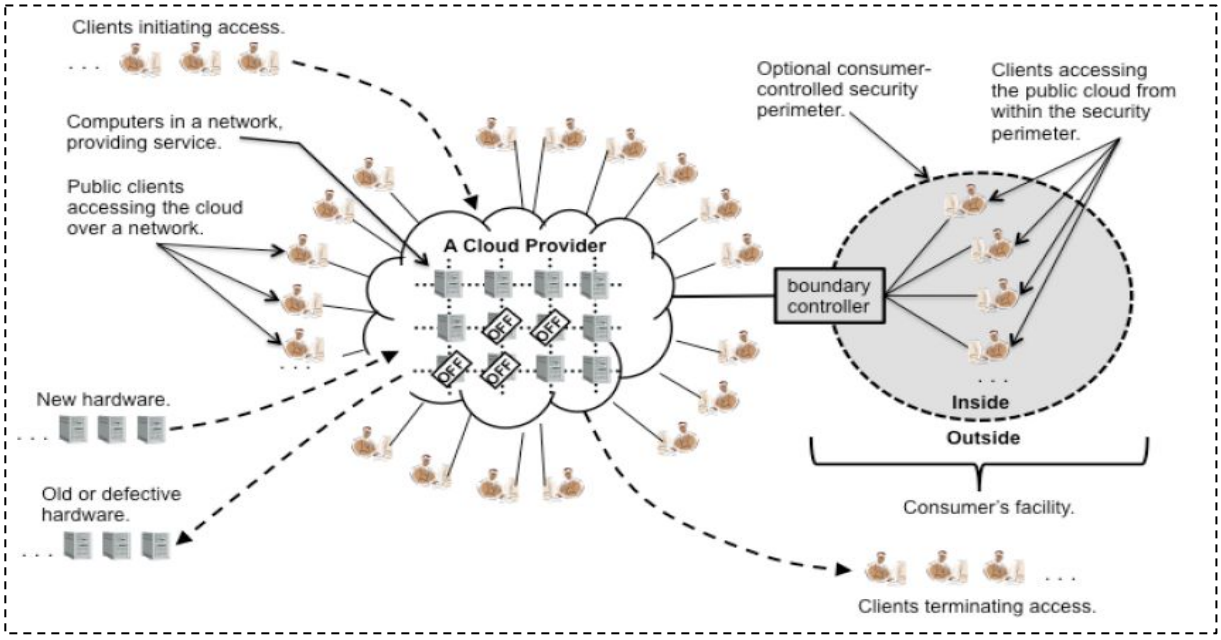
a) Le modèle public

i) Fonctionnement et caractéristiques

- Fonctionnement

L'infrastructure du modèle public est offerte par un prestataire de services dont l'utilisation est ouverte au public. Le modèle peut appartenir, être géré et être opéré par une entreprise, une institution, une organisation gouvernementale ou une combinaison de ceux-ci[29].

Figure 1 : Fonctionnement du modèle public[30]



- Services offerts

Généralement, les services sont utilisés via Internet, ce qui implique que le traitement des données aura lieu à l'extérieur du coupe-feu[31] de l'entreprise[32]. Les services peuvent être

[29] P. MELL et T. GRANCE, préc., note 8.

[30] L. BADGER *et al.*, préc., note 18, p. 4-14.

[31] Aussi dénommé « pare-feu », un « coupe feu » est défini comme étant un « dispositif informatique qui permet le passage sélectif des flux d'information entre deux réseaux, ainsi que la neutralisation des tentatives de pénétration extérieures ». Voir OLF, préc., note 3.

[32] John RHOTON, David GRAVES et Jan DE CLERCQ, *Cloud Computing Protected*, USA, Recursive Press, 2013.

gratuits[33] ou payants. Mentionnons, par exemple, les services de stockage de photos en ligne, les services de courriel ou les sites de réseautage social. De plus, les services sont normalement offerts à une grande variété de clients.

ii) Avantages et inconvénients

- *Avantages*

Selon le NIST, la réduction des coûts et l'augmentation de l'efficience sont les premiers motifs justifiant le recours au modèle public[34]. Par ailleurs, ce modèle offrirait aux utilisateurs une illusion de ressources illimitées, puisqu'il ne comporte généralement pas de restrictions quant aux capacités de localisation et de stockage. En plus d'être élastique, le modèle public comporte une grande flexibilité de mouvement des charges de travail correspondant aux ressources disponibles, et les utilisateurs peuvent utiliser les services de manière conjointe avec d'autres sans être limités par des périmètres de sécurité statiques[35]. En effet, l'un des principaux arguments relatifs à l'économie du nuage est que les centres de données, et donc les charges de travail, peuvent être localisés là où les coûts sont les plus bas. Ainsi, un prestataire peut faire migrer les charges de travail d'un utilisateur à n'importe quel moment, à moins que le prestataire ait offert des conditions d'emplacement spécifiques et que le client ait configuré son compte de manière à pouvoir demander des restrictions de localisation. Toutefois, le client ne dispose généralement pas des moyens nécessaires afin de vérifier si les emplacements convenus sont respectés[36].

- *Inconvénients*

Les utilisateurs des services fournis par le modèle public vont dépendre du bon fonctionnement du réseau Internet sur lequel ils se connectent pour accéder à ceux-ci. Un problème sur le réseau tel qu'une mauvaise configuration, une panne ou une attaque compromettra la fourniture des

---

[33] La gratuité est toutefois relative puisque ces services se réservent certains droits quant à l'utilisation des contenus. Voir *infra*, p. 132.

[34] W. JANSEN et T. GRANCE, préc., note 27, p. 6.

[35] L. BADGER *et al.*, préc., note 18, p. 4-14.

[36] *Id*.

services[37]. De ce fait, l'infonuagique publique s'expose davantage aux cyberattaques et autres menaces.

Par ailleurs, le manque de transparence que comporte le modèle public entraîne une perte de contrôle et de visibilité sur la sécurité des données stockées dans le nuage. En effet, les détails concernant le système opérationnel ne sont en principe pas divulgués aux utilisateurs et, dans la plupart des cas, les logiciels employés pour fournir le service ne peuvent être accessibles pour examen. Conséquemment, les utilisateurs ne disposent pas de garanties qu'ils pourront contrôler leurs ressources stockées dans le nuage[38].

Une autre incidence importante liée au modèle public est que les connaissances et l'expertise interne en matière d'infonuagique profiteront généralement au prestataire de services. Avec le temps, l'utilisation du modèle public a pour effet de diminuer le niveau de connaissances et d'expertise au sein de l'organisation cliente, puisque l'équipe interne n'a plus à gérer les problèmes techniques liés aux services offerts par le nuage. À moins que des précautions ne soient prises, une organisation peut ainsi « perdre sa capacité de se tenir à jour des progrès technologiques et des conditions de sécurité et de confidentialité liés à ceux-ci »[39]. Ceci peut affecter sa capacité à planifier de nouveaux projets technologiques et à superviser les systèmes infonuagiques existants de façon efficace[40].

Finalement, le risque pour la sécurité des données est susceptible d'augmenter lorsque le prestataire de services infonuagiques impartit à son tour le traitement des données, le stockage ou l'archivage, si aucune disposition contractuelle n'a été prévue à l'effet contraire.

---

[37] *Id*.

[38] *Id.* [TRADUCTION] « [...] Bien que certains fournisseurs puissent faire des efforts pour faire respecter les requêtes des consommateurs et que d'autres puissent fournir des services de surveillance, les consommateurs doivent avoir confiance que le fournisseur remplit ses fonctions fidèlement ou, si le fournisseur a contracté avec une tierce-partie, que celui-ci fait des vérifications précises et en temps opportun. À titre d'exemple, il n'est actuellement pas possible pour le consommateur de vérifier que l'information a été entièrement supprimée des systèmes du fournisseur ».

[39] W. JANSEN et T. GRANCE, préc., note 27, p. 40.

[40] *Id*., p. 40.

À retenir…

Le manque de transparence que comporte le modèle public entraîne une perte de contrôle et de visibilité sur la sécurité des données stockées dans le nuage. De plus, il s'expose davantage aux risques de cyberattaques. Le scénario le moins risqué pour le gouvernement serait donc qu'il emploie ce modèle pour les données publiques uniquement. Si, toutefois, des renseignements sensibles devaient tout de même circuler dans ce système, des mesures de sécurité appropriées devraient être mises en place, telles que des technologies de chiffrement, de manière à assurer la protection des renseignements personnels et confidentiels. Notons qu'il devrait être tenu compte des conditions dans lesquelles les renseignements chiffrés seront traités, le cas échéant, des années plus tard, afin de s'assurer que le gouvernement pourra déchiffrer les données dans le futur.

b) Le modèle privé

L'infonuagique privée est un modèle de déploiement dont l'infrastructure est dédiée exclusivement à une organisation ou à une entreprise spécifique. Elle peut être exploitée par l'organisation même (dans quel cas elle sera opérée soit à l'interne, soit à l'externe[41]) ou un intermédiaire[42]. Pour cette raison, la notion même d'un nuage privé fait l'objet d'une remise en question par certains spécialistes puisqu'il ne s'agirait, en fait, que d'une extension des fonctionnalités déjà offertes par un centre informatique[43][44]. Ceci étant, puisque l'expression demeure répandue[45] et par souci d'exhaustivité, nous en ferons l'analyse.

Le modèle privé a le potentiel de fournir à l'organisation plus de contrôle que l'infonuagique publique sur l'infrastructure, les ressources computationnelles et les utilisateurs du nuage[46]. Le

[41] L. BADGER *et al.*, préc., note 18, p. 4-2.

[42] W. JANSEN et T. GRANCE, préc., note 27, p. 3.

[43] « Service équipé de matériel informatique et péri-informatique, qui regroupe des travaux de traitement de l'information de toute nature pour le compte des autres services au sein d'une entité ou d'une entité cliente ». Voir OLF, préc., note 3.

[44] J. RHOTON, J. De CLERC et D. GRAVES, préc., note 32, p. 9.

[45] Elle figure notamment dans le rapport du NIST. Voir P. MELL et T. GRANCE, préc., note 8.

[46] *Id.*, p. 3.

modèle privé s'apparenterait aux services offerts par les prestataires de services d'hébergement traditionnels et permettrait de connaître précisément l'emplacement géographique des données[47].

Par ailleurs, ce modèle offrirait plusieurs avantages pour la visibilité, la fiabilité, la protection des ressources et la productivité. En effet, la gestion est davantage intégrée dans l'environnement informatique, ce qui signifie qu'il est « possible de mettre en place des normes, des procédures et un contrôle plus précis, plus faciles à surveiller, à auditer et à appliquer. L'administration et la gouvernance en sont simplifiées et améliorées d'autant »[48].

La séparation logique et physique que comporte le modèle privé permettrait à celui-ci d'optimiser les capacités de résistance et de tolérance aux pannes informatiques[49]. De cette manière, « en cas d'échec en local, les applications peuvent automatiquement migrer vers les ressources voisines qui sont disponibles. Les sauvegardes (ainsi que l'ajustement du degré de redondance) peuvent être plus robustes. De plus, les procédures de restauration sont plus complètes, car l'administrateur a moins souvent besoin de restaurer physiquement les machines (restaurations depuis des bandes, permutations de disques, etc.) »[50].

Sous le modèle privé, les mesures de sécurité qui sont déjà utilisées dans une organisation peuvent normalement être étendues dans l'environnement infonuagique. Ainsi, une organisation peut imbriquer les règles relatives à l'accès, à l'utilisation, à l'emplacement et à la gestion de ses ressources. En outre, « si elle combine cet effort avec la gestion des identités et autorisations associées aux individus, l'entreprise bénéficie d'une protection plus granulaire, plus précise, plus transparente et plus facile à gérer. Elle peut ainsi étendre davantage de procédures de contrôle de la sécurité sur un plus grand nombre de ressources »[51]. De cette manière, l'organisation peut plus

[47] EMC^2, « Créer un cloud sécurisé : stratégies de déploiement des clouds privés et hybrides », en ligne : < http://france.emc.com/collateral/emc-perspective/h8558-cloud-trust-ep.pdf >, p. 6.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

facilement se conformer aux règles relatives à la protection des renseignements et être en mesure de démontrer les mesures prises à cet effet.

L'utilisation du modèle privé faciliterait par ailleurs l'accès aux données par les employés qui utilisent les services, ayant pour effet d'influencer leur niveau de productivité. Aussi, ce modèle rend « plus productives la fourniture, la consommation et la gestion des services technologiques »[52]. Par exemple, « les ressources technologiques peuvent être définies et assemblées différemment, au moyen de méthodes telles que la gestion des métadonnées et la virtualisation »[53].

Notons que le modèle privé peut être envisagé de deux façons distinctes, soit le modèle privé interne (i) et le modèle privé externe (ii).

i) Le modèle privé interne

- *Fonctionnement et caractéristiques*

Fonctionnement

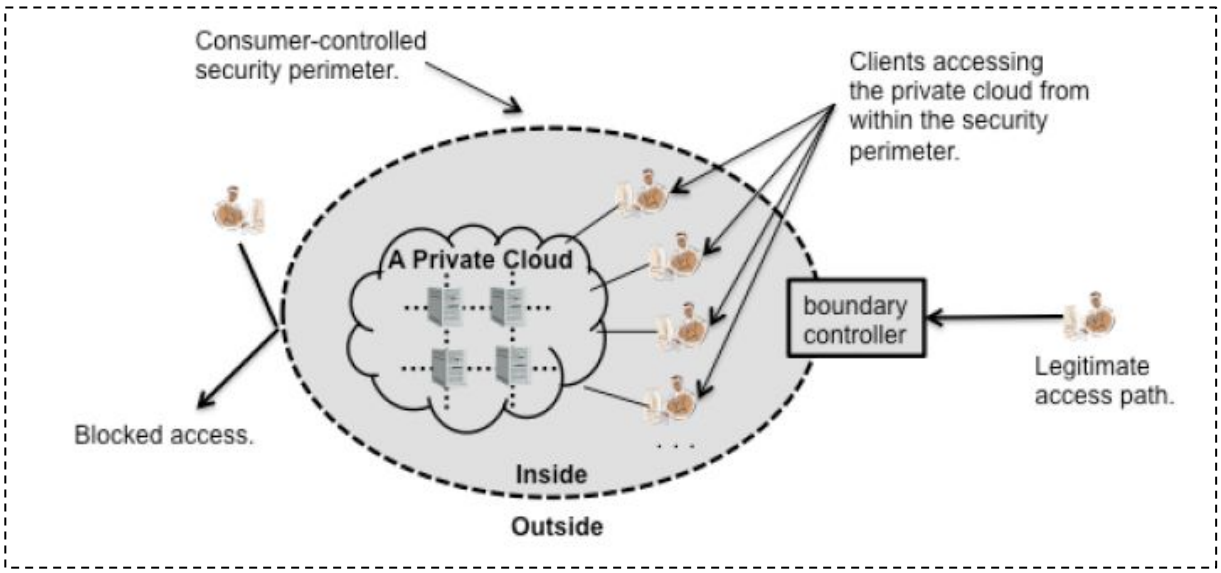
Selon le modèle privé interne, les logiciels de gestion du système sont installés à l'intérieur de l'organisation. Le périmètre de sécurité s'étend à la fois autour des ressources informatiques internes du client et des ressources du prestataire. Le nuage peut être centralisé sur un seul emplacement du client ou, encore, être distribué sur de multiples emplacements. Le périmètre de sécurité du client existera seulement s'il est mis en place par celui-ci, mais il ne garantit pas le contrôle sur les ressources du modèle privé. Son existence permet néanmoins au client d'exercer un certain contrôle sur les ressources confiées à l'interne[54].

[52] *Id.*, p. 11.

[53] *Id.*

[54] L. BADGER *et al.*, préc., note 18, p. 4-4.

Figure 2 : Fonctionnement du modèle privé interne[55]



Services offerts

Les services peuvent être administrés directement par l'organisation, ou en collaboration avec un prestataire de service qui prend en charge une partie des services externalisés. L'organisation qui décide de gérer elle-même ses infrastructures informatiques et ses centres de données devra fournir les ressources afin de répondre à ses différents besoins ou services[56].

- Avantages et inconvénients

Avantages

Avec le modèle privé interne, les problèmes de dépendance au réseau peuvent être limités aux ressources sur lesquelles l'utilisateur a le contrôle, selon la configuration du réseau mis en place. De ce fait, les difficultés liées à la congestion d'Internet ou à la communication avec le *Domain Name System* (« DNS »)[57] peuvent être évitées[58]. Cependant, si le client possède plusieurs sites

[55] *Id.*

[56] EMC², préc., note 47, p. 6.

[57] Le *Domain Name System* (en français, le système de noms de domaine) est défini comme étant un « système distribué de bases de données et de serveurs, qui assure la traduction des noms de domaine utilisés par les internautes

physiques et souhaite détenir de multiples accès au même service, il doit s'assurer que les sites sont sécurisés, afin d'en prévenir les divergences[59].

Pour se protéger des menaces extérieures à son système**,** le client a la possibilité de régler le périmètre de sécurité de la même manière qu'un système informatique traditionnel. Le niveau de sécurité peut donc être équivalent à celui-ci[60].

Au final, le client choisit l'infrastructure sur laquelle le modèle opère et détermine ainsi l'emplacement géographique des charges de travail. Même si certains utilisateurs individuels peuvent ne pas savoir où se trouvent physiquement leurs charges de travail dans l'infrastructure interne de l'organisation à un moment donné, le client détient une visibilité et un contrôle sur l'emplacement où celles-ci sont autorisées[61].

Inconvénients

D'une part, le recours au modèle privé interne requiert des compétences approfondies en technologie de l'information afin de gérer les dispositifs permettant d'accéder au système, tant lors de son inauguration que par la suite. Ainsi, une équipe en TI devra gérer les contrats de

---

en numéros Internet utilisables par les ordinateurs, ceci pour permettre la transmission des messages d'un site à l'autre du réseau ». Voir OLF, préc., note 3.

[58] L. BADGER *et al.*, préc., note 18, p. 4-5.

[59] *Id*. [TRADUCTION] « [...] si une organisation cliente possède plusieurs sites physiques et désire que chaque site ait accès au même nuage privé, elle doit soit fournir un outil qui sert à la communication entre les différents sites, tel qu'une ligne cryptée louée, soit utiliser la cryptographie (par ex. avec un VPN) par le biais de réseaux moins protégés tel qu'Internet. Ces options présentent toutes deux des risques pour la disponibilité et pour la sécurité, car le bon fonctionnement du réseau dépendra de ressources qui ne sont pas directement contrôlées par le client et tout échec dans l'application et dans la configuration des mécanismes cryptographiques peut permettre l'accès à des tiers. Le client doit également s'assurer que les sites sont protégés par un niveau de sécurité approprié ou que des barrières de sécurité soient installées pour éviter des fluctuations dans les niveaux de sécurité ».

[60] L. BADGER *et al.*, préc., note 18, p. 4-6 : [TRADUCTION] « Dans le modèle privé interne, l'utilisateur a l'option d'implanter un périmètre de sécurité assez vigoureux, pouvant atteindre le même niveau de sécurité que pour les ressources qui ne sont pas liées à l'infonuagique, afin de protéger ses ressources contre les menaces externes. Quant au traitement de l'information qui n'est pas nécessairement sensible, le périmètre de sécurité peut être construit en utilisant un pare-feu commercial et des réseaux privés virtuels. Quant à l'information qui est plus sensible, le périmètre de sécurité peut être construit en utilisant un pare-feu avec une politique plus restrictive [Zwi00, Ran99], une authentification multifactorielle [SP-800-63], le cryptage [Sch94, Ros99], la détection et la prévention des intrusions et même l'isolement physique ».

[61] *Id*.

licence, l'équipement et les besoins du système en sécurité et en projets spéciaux. En outre, des compétences additionnelles pour opérer un système infonuagique seront requises (par exemple, en matière de conservation de données dans le nuage pour les organisations traitant une grande quantité de renseignements[62]).

D'autre part, les charges de travail de différents clients peuvent résider de manière concurrente sur une même architecture logicielle partagée ou sur un réseau local, séparés uniquement par des politiques d'accès implantées au moyen d'un logiciel. Un défaut dans la mise en place des politiques d'accès du prestataire pourra compromettre la sécurité de l'organisation en exposant ses charges de travail à d'autres clients. Ainsi, il peut en découler une confusion et une divulgation non autorisée de renseignements confidentiels et de données relatives à la propriété intellectuelle, par exemple. Le modèle privé peut toutefois atténuer ce risque, puisque le nombre d'attaques potentielles est moins élevé et les utilisateurs seront généralement des membres de l'organisation cliente ou des partenaires autorisés. Le NIST précise toutefois que :

> [TRADUCTION] « […] le modèle reste vulnérable aux attaques qui peuvent être conduites par des initiés autorisés et malveillants. Différentes fonctions organisationnelles, telles que le service de paie, le stockage de renseignements personnel ou la propriété intellectuelle, peuvent être combinées à la suite de telles failles de sécurité et ainsi permettre aux utilisateurs non autorisés d'accéder à et, éventuellement, de divulguer l'information se trouvant dans le nuage interne ».[63]

Il importe de mentionner que la performance de l'échange de données dans le modèle interne reste limitée aux capacités du réseau de l'organisation cliente. Toutefois, les limites imposées par le réseau peuvent être ajustées, sans être éliminées, en mettant à la disposition de l'organisation une interconnexion de réseaux plus performants et/ou plus fiables à l'intérieur de son infrastructure[64]. Notons par ailleurs que les ressources seront généralement limitées dans l'utilisation d'un modèle privé interne. En effet, celui-ci dispose d'une capacité informatique et

---

[62] *Id.*, p. 4-5.

[63] *Id.*, p. 4-6.

[64] *Id.*

de stockage fixe en fonction de charges de travail anticipées et de restrictions de coûts[65]. Par contre, si une organisation est assez vaste et supporte une diversité de charges de travail, le modèle peut fournir une bonne élasticité aux utilisateurs à l'interne[66]. Un modèle plus réduit expose toutefois une capacité maximale similaire à celle des centres de données traditionnels. Ajoutons que, d'ordinaire, le modèle privé interne nécessite que certains coûts soient acquittés d'avance[67].

Pour finir, la migration des données peut entraîner des coûts importants pour l'organisation cliente en raison, notamment, des applications de gestion du système qui devront, en principe, être installées sur son équipement informatique[68].

ii) Le modèle privé externe

- Fonctionnement et caractéristiques

Le modèle privé externe est exploité par une tierce partie au bénéfice d'une organisation, et les serveurs sont normalement situés à l'extérieur des locaux de celle-ci. Le système dispose de deux périmètres de sécurité, l'un étant implanté par le client et l'autre par le prestataire. La sécurité des données et du traitement dépendra de la force et de la disponibilité des périmètres de sécurité, ainsi que de la sécurisation de la connexion entre les deux. Ainsi, le prestataire se doit de renforcer le périmètre de sécurité mis en place et d'éviter que le système du client ne soit confondu avec d'autres ressources infonuagiques externes à celui-ci. La force du périmètre de sécurité du prestataire dépendra des conditions établies au préalable par le client[69].

---

[65] *Id*., p. 4-7.

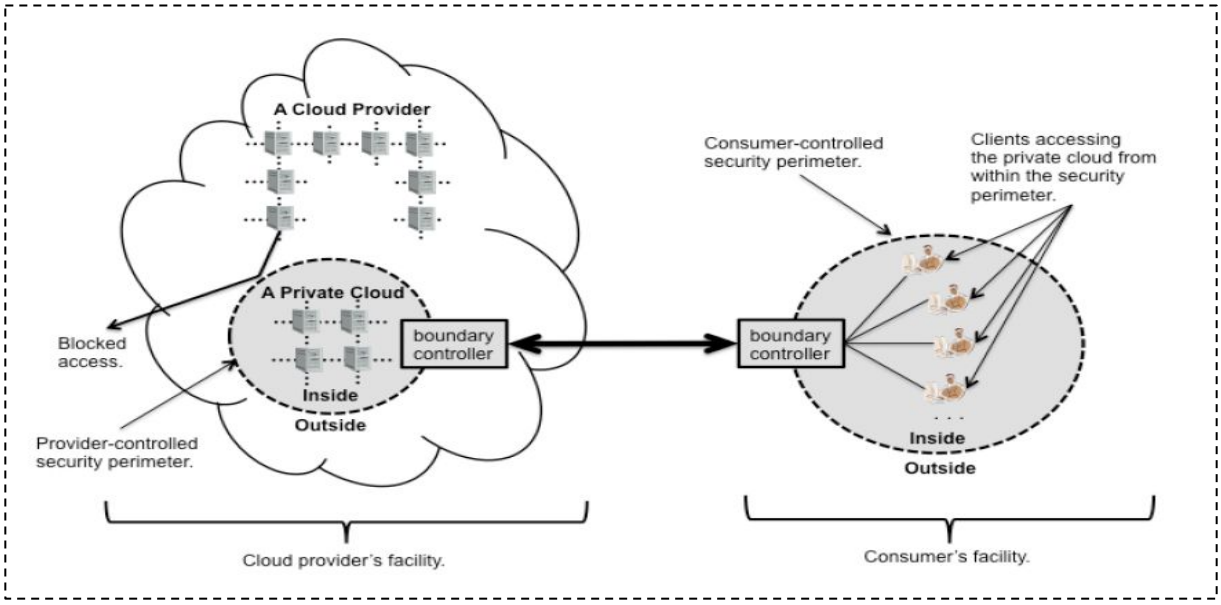
[66] *Id.,* p. 4-7.

[67] *Id*.

[68] *Id*., p. 4-6 : [TRADUCTION] « Si le nuage est supposé supporter des charges de travail procédurales ou informationnelles intensives, le logiciel devra être installé sur plusieurs systèmes bas de gamme ou sur un nombre limité de systèmes plus performants. L'installation de logiciels infonuagiques et la gestion des installations encoure généralement des coûts initiaux significatifs, même si le logiciel est gratuit et même si la plupart du matériel informatique existe déjà dans l'organisation cliente ».

[69] *Id*., p. 4-7.

Figure 3 : Fonctionnement du modèle privé externe[70]



- Avantages et inconvénients

Avantages

Tout comme pour le modèle privé interne, le modèle privé externe a l'avantage de proposer une grande transparence et un contrôle élevé, notamment quant à l'emplacement et l'isolation des ressources[71]. En effet, le modèle privé externe offre la possibilité aux utilisateurs d'une même organisation d'exercer un certain contrôle sur l'emplacement des données. En présumant que le prestataire implante le périmètre de sécurité de la manière désignée par le client, les données se déplacent uniquement à l'intérieur de ce périmètre[72]. De plus, les utilisateurs détiennent l'option que soient mis à leur disposition des liens de communication protégés et fiables avec le prestataire[73].

[70] L. BADGER *et al.*, préc., note 18, p. 4-8.

[71] EMC^2, préc., note 47, p. 3.

[72] L. BADGER *et al.*, préc., note 18, p. 4-8.

[73] *Id.*

Contrairement au modèle interne, où les ressources doivent être fournies d'avance, le client du modèle privé externe peut louer les ressources selon la quantité offerte par le prestataire[74]. D'ailleurs, la fourniture et l'opération d'équipements informatiques « à l'échelle » figurent parmi les compétences clés des prestataires[75].

Le modèle externe dispose d'une capacité fixe à un moment donné et l'élasticité offerte aux clients peut être effective seulement si le système infonuagique est assez étendu et que les charges de travail sont assez diversifiées. Aussi, et pareillement au modèle interne, le modèle externe exposera une capacité maximale équivalente à celle des centres de données traditionnels[76].

Inconvénients

La principale différence entre le modèle privé interne et le modèle privé externe est que, dans le second cas, les mesures doivent être appliquées sur les deux périmètres de sécurité, celui du client et celui du prestataire. De plus, des mesures de sécurité doivent être mises en place pour protéger les communications entre les deux périmètres[77]. Ainsi, bien qu'une variété de mesures permette de protéger les périmètres de sécurité des menaces provenant de l'extérieur, il demeure que les risques de failles de sécurité sont doublés.

Les risques quant à la performance limitée de l'échange de données sont équivalents au modèle privé interne. La performance limitée par le réseau peut aussi être ajustée par le prestataire, mais ceci nécessite un contrat particulier et engendre des coûts supplémentaires significatifs[78]. Par ailleurs, les risques liés aux emplacements multiples des données sont les mêmes que sous le modèle privé interne.

---

[74] *Id.,* p. 4-9.

[75] *Id.*

[76] *Id.*

[77] *Id*.

[78] *Id*.

À retenir…

Dans le modèle privé interne, les ressources demandées sont installées à l'intérieur de l'organisation cliente et requièrent que le client possède les compétences nécessaires en technologie de l'information pour gérer les dispositifs lui permettant d'accéder au système, tant lors de son inauguration que lors de son fonctionnement. De ce fait, le gouvernement disposerait d'un plus grand contrôle sur ses ressources et ses données, notamment en raison du fait qu'il connaît l'emplacement de ses serveurs et de ses charges de travail. Ainsi, les principales menaces découlant de l'utilisation de ce modèle se trouveront à l'interne de l'organisation. Par conséquent, les politiques internes d'accès devront être soigneusement mises en œuvre par le gouvernement et ses agences.

Dans le modèle externe, les ressources sont confiées et gérées à l'extérieur de l'organisation. De ce fait, les mesures de sécurité doivent être appliquées sur les deux périmètres de sécurité, celui du client et celui du prestataire. De plus, des mesures de sécurité doivent être mises en place pour la protection des communications entre les deux périmètres.

c) Le modèle communautaire

i) Fonctionnement et caractéristiques

- *Fonctionnement*

Apparenté à l'infonuagique privée, le modèle communautaire est partagé par plusieurs organisations ayant les mêmes besoins et est mis à la disposition de ces groupes uniquement. Les organisations peuvent exploiter elles-mêmes les services, les déléguer à une tierce partie ou les exploiter conjointement. Ainsi, le modèle communautaire peut être interne ou externe, et serait « similaire au modèle privé, mais l'infrastructure et les ressources informatiques sont fournies exclusivement à deux organisations ou plus détenant des politiques similaires quant à la confidentialité, la sécurité et la réglementation ».[79]

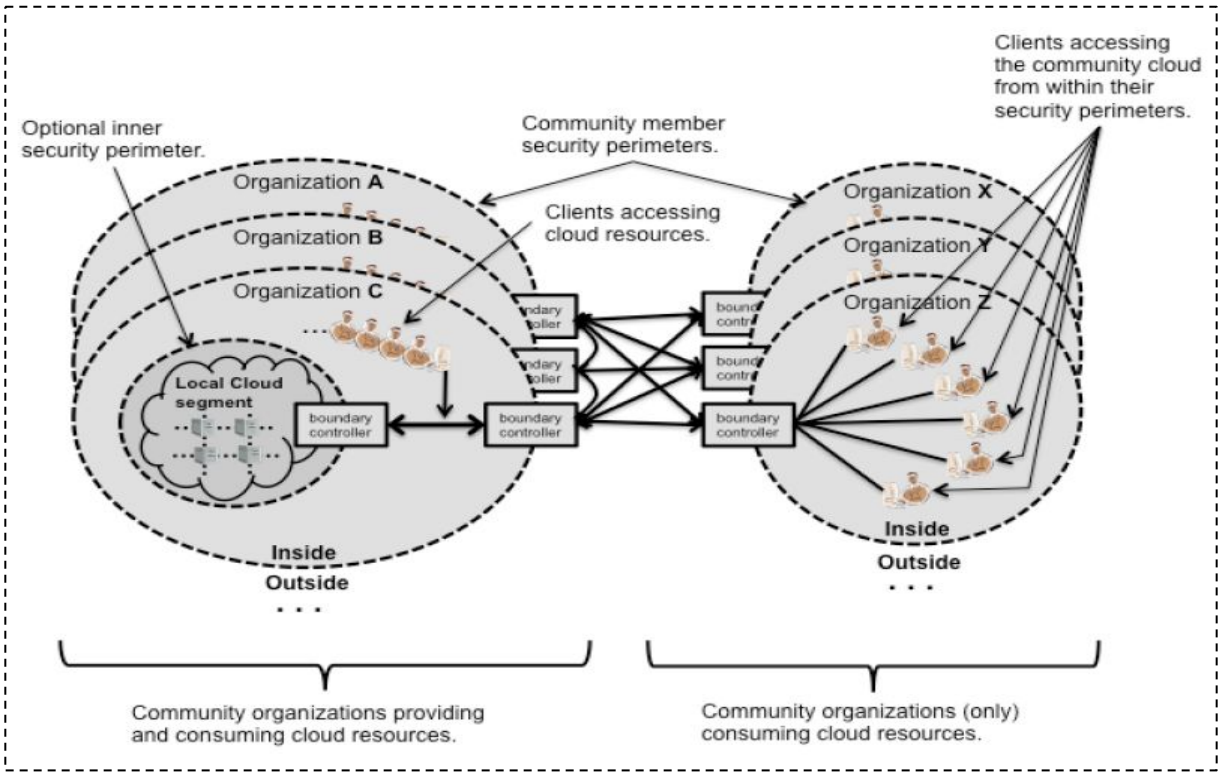
En présumant que chaque organisation détient son propre périmètre de sécurité, les utilisateurs du modèle communautaire interne se connectent par le biais de liens de communication entre les limites de contrôle qui permettent l'accès à travers leurs périmètres de sécurité. Les organisations pourront également implanter un périmètre supplémentaire afin d'isoler les ressources infonuagiques des autres ressources locales. En effet :

[79] W. JANSEN et T. GRANCE, préc., note 27, p. 3.

> [TRADUCTION] « Peu importe la configuration, les barrières de sécurité devraient permettre l'accès aux ressources infonuagiques aux clients locaux ainsi qu'aux clients d'autres organisations participantes. Toutefois, fournir l'accès aux ressources infonuagiques locales ne devrait pas accorder l'accès aux ressources non infonuagiques, à moins que l'octroi d'un tel accès soit un objectif spécifique de l'organisation ».[80]

De façon similaire au modèle privé externe, les responsabilités du côté serveur sont gérées par un prestataire de services qui implante le périmètre de sécurité et qui empêche que les ressources des communautés soient confondues avec d'autres ressources provenant de l'extérieur. La principale nuance avec le modèle privé est que le prestataire se doit d'appliquer des politiques partagées parmi les organisations utilisatrices du système communautaire[81].

Figure 4 : Fonctionnement du modèle communautaire interne[82]

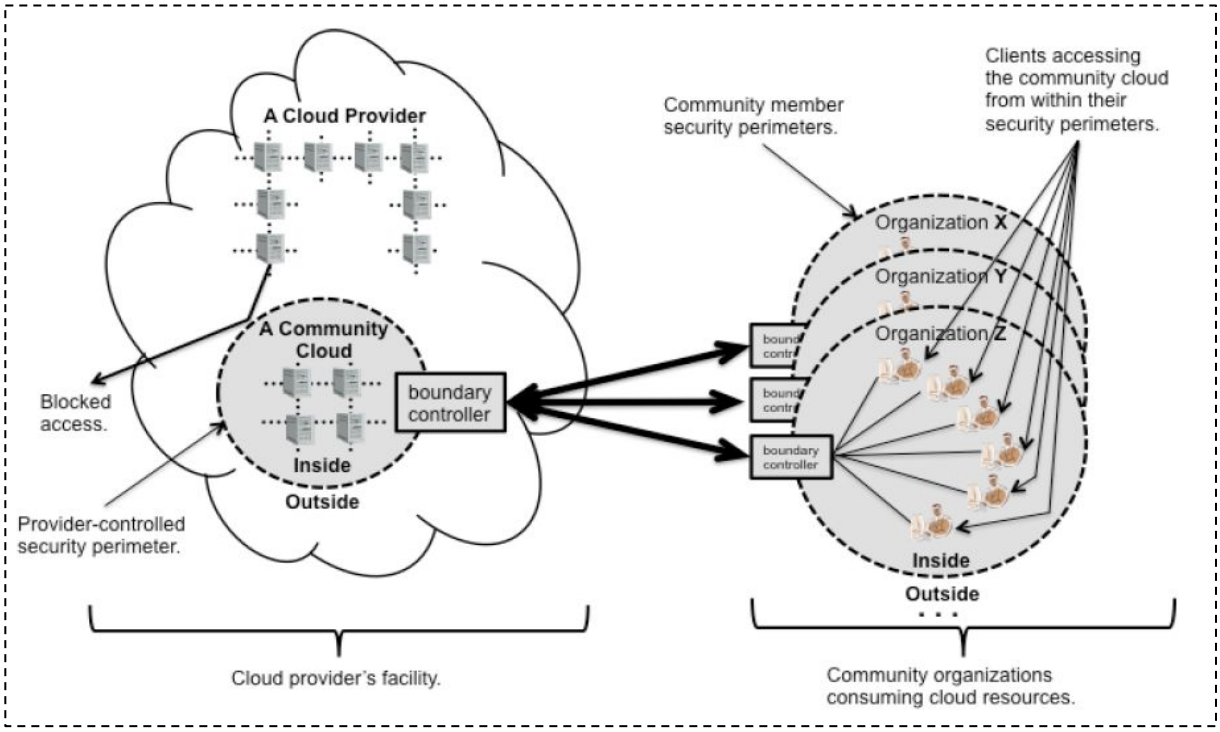


[80] L. BADGER *et al.*, préc., note 18, p. 4-9.

[81] *Id.,* p. 4-12.

[82] *Id.*, p. 4-10.

Figure 5 : Fonctionnement du modèle communautaire externe[83]



- Services offerts

L'exemple le plus commun est celui de l'infonuagique gouvernementale ouverte aux différents ministères et organismes[84]. D'autres avantages s'offrent également aux entreprises désirant travailler ensemble et/ou mettre leurs ressources en commun.

ii) Avantages et inconvénients

- *Avantages*

Des organisations œuvrant dans un même secteur auront souvent un encadrement législatif similaire. De ce fait, elles ont intérêt à mettre en commun leurs ressources afin de réduire les coûts liés à la gestion et à la sécurité du système.

---

[83] *Id.*

[84] J. RHOTON, J. De CLERC et D. GRAVES, préc., note 32, p. 12.

- Inconvénients

La plupart des inconvénients expliqués dans le scénario privé externe se retrouvent dans le scénario communautaire externe. Les risques liés à une connexion partagée sont donc les mêmes que pour le modèle privé, de même que les limitations de performance de l'échange de données. De plus, les problèmes de dépendance au réseau sont semblables à ceux expliqués dans le scénario privé externe. La principale différence est qu'il peut y avoir de nombreux liens de communication entre les membres de la communauté et les installations du prestataire[85]. Ainsi, le niveau de sécurité du modèle communautaire dépendra principalement de la force des mesures déployées sur les périmètres de sécurité et les liens de communication[86].

L'infonuagique communautaire interne possède deux catégories de participants, soit ceux qui fournissent les services infonuagiques à la communauté et ceux qui utilisent les ressources infonuagiques. Pour l'organisation qui fournit les services, les connaissances requises en TI pour l'exploitation du système seront similaires à celles requises pour le modèle privée interne, sauf que l'ensemble de la configuration du nuage peut être plus complexe et requerra un niveau de compétences plus élevé[87]. Pour l'organisation utilisatrice, les habiletés nécessaires seront plus grandes au niveau des configurations si les services sont fournis par plus d'un prestataire[88]. De la sorte, il peut être difficile de gérer les contrôles d'identité et les accès des organisations participantes. Dans tous les cas, il sera essentiel que les organisations du système communautaire négocient des politiques claires d'accès aux ressources[89].

[85] L. BADGER *et al.*, préc., note 18, p. 4-12.

[86] *Id.*

[87] *Id.*, p. 4-11.

[88] *Id.*

[89] *Id.*

À retenir…

Le modèle communautaire est apparenté au modèle privé et servira à combler les besoins des organismes voulant mettre en commun leurs ressources. Les organismes peuvent exploiter eux-mêmes les services, les déléguer à une tierce partie ou les exploiter conjointement. Au niveau de la sécurité, la principale différence entre le modèle privé et le modèle communautaire est que, pour le modèle communautaire, le prestataire doit mettre en vigueur des politiques partagées parmi les organisations utilisatrices du système communautaire. Notons également que la configuration du nuage communautaire interne peut être complexe et requerra un niveau de compétences plus élevé. En effet, il peut être difficile de gérer les contrôles d'identité et les accès des organismes participants. Dans tous les cas, il sera essentiel que les participants du système communautaire négocient des politiques claires d'accès aux ressources.

d) Les modèles hybrides

i) Fonctionnement et caractéristiques

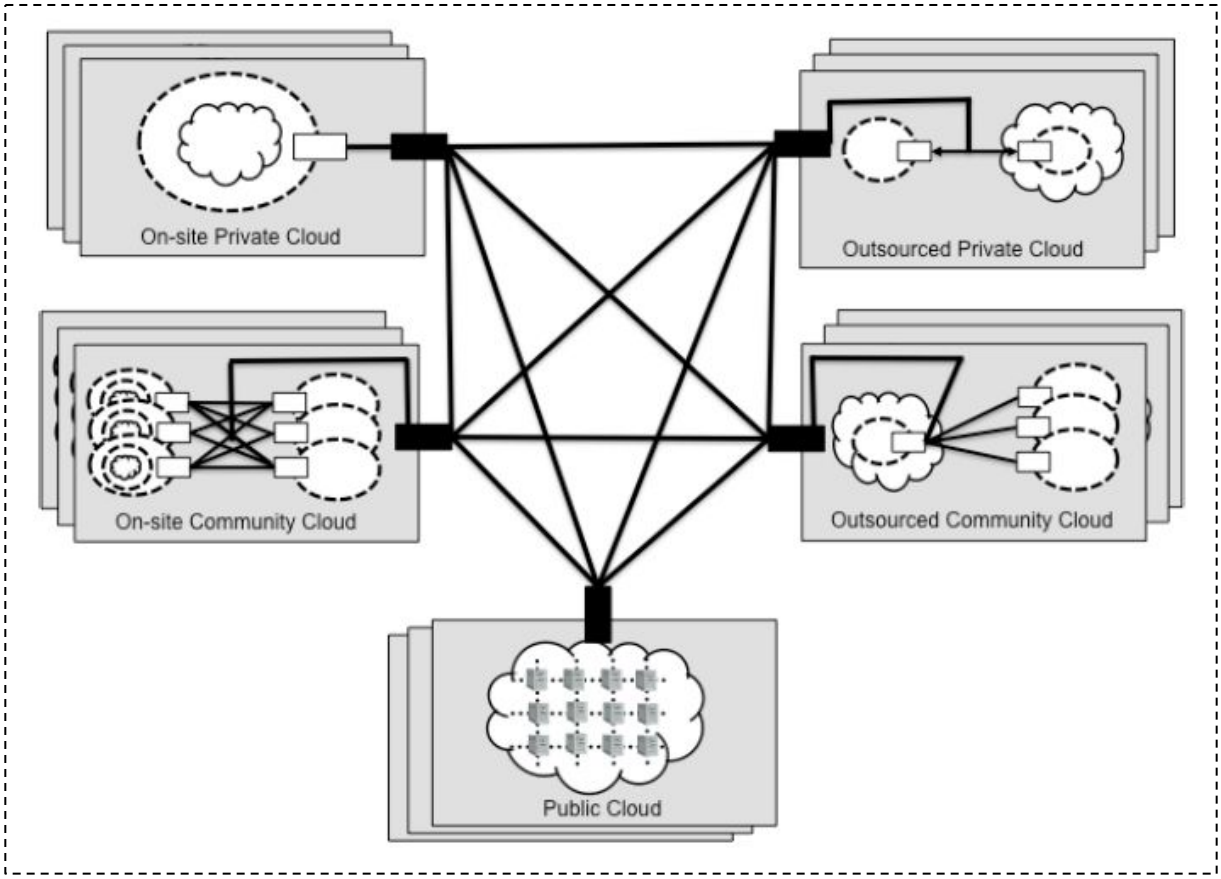
- *Fonctionnement*

Le modèle hybride serait le plus complexe des modèles de déploiement, puisqu'il implique généralement une combinaison de deux ou plusieurs modèles (privé, public et/ou communautaire), selon les besoins de l'organisation[90]. Par exemple, des conditions propres à une entreprise ou une catégorie particulière de données nécessiteront la mise en place de services virtuels basés sur des modèles à la fois public et privé[91]. Il découle de ce qui précède qu'il serait préférable de parler de plusieurs modèles hybrides que d'un seul modèle hybride vu les multiples variations possibles. Évidemment, puisqu'il existe un nombre illimité de modèles hybrides, nous limiterons notre analyse aux points communs à l'ensemble de ces modèles.

[90] *Id.*, p. 4-16.

[91] Voir EMC[2], préc., note 47 ; L. BADGER *et al.*, préc., note 18; et SYNTEC NUMÉRIQUE, préc., note 10.

Figure 6 : Fonctionnement du modèle hybride[92]



- Services offerts

Les modèles hybrides offrent une portabilité des données et des applications[93] et permettent une grande flexibilité dans l'exploitation des ressources et des charges de travail. En effet, les ressources internes et externes peuvent être combinées afin de permettre un environnement dans lequel « les ressources externes seraient sollicitées dès que les ressources internes atteindraient leurs limites (souvent appelé "cloudbursting") »[94].

[92] L. BADGER *et al.*, préc., note 18, p. 4-15.

[93] *Id.*

[94] Erik VAN OMMEREN *et al.*, « Maîtrisez le cloud », (2011) IBM & Sogeti, en ligne : < http://www.fr.sogeti.com/sites/default/files/Documents/Publications/SOGETI_Maitrisez-leCloud.pdf >, p. 40.

Ainsi, dès que le potentiel de stockage des données à l'interne est atteint, le système de stockage du modèle privé externe est immédiatement appelé en renfort. Un scénario hybride implique donc une couche de gestion et d'intégration supplémentaire[95]. Il s'agit, encore une fois, d'un exemple parmi tant d'autres des types de services offerts par les modèles hybrides.

ii) Avantages et inconvénients

Avantages

L'adaptation des modèles aux besoins des organisations permet à celles-ci d'en tirer les avantages propres à chacun. Tel que mentionné, les modèles hybrides permettent aux entreprises de tirer le meilleur parti de chaque type de nuage[96]. Les charges de travail peuvent ainsi se répartir de deux manières principales entre les nuages public et privé : « lorsque les données se déplacent entre une application d'un cloud public et les bases de données et applications d'un cloud privé, et lorsque les serveurs et le stockage d'un cloud public jouent le rôle de suppléments à la demande pour les ressources de cloud privé, en cas de pic d'utilisation. L'entreprise doit étudier et aborder avec soin la gestion de ces échanges entre clouds, qui ajoute à la complexité existante »[97].

Si l'on prend l'exemple de la combinaison public-privé, l'idéal est de « pouvoir conjuguer les atouts de ces deux univers, à savoir de pouvoir accéder aux services innovants et à la demande du cloud public tout en conservant la maîtrise de la gestion comme c'est le cas dans un cloud privé »[98]. L'approche combinée du modèle hybride permet ainsi d'apporter une grande flexibilité dans l'utilisation des ressources.

---

[95] *Id*.

[96] EMC^2, préc., note 47, p. 7.

[97] *Id*.

[98] EMC^2, « Le cloud privé et ses avantages métiers : des coûts réduits et une réactivité accrue », (2010), en ligne : < http://france.emc.com/collateral/emc-perspective/h6870-consulting-cloud-ep.pdf >, p. 9.

Inconvénients

Comme le mentionne le NIST, la configuration des services infonuagiques hybrides peut être extrêmement complexe[99]. En outre, les politiques de sécurité régissant les flux d'information et l'accès aux ressources peuvent être mises en place de plusieurs manières, et les enjeux liés à la gestion des identités ne sont pas nécessairement connus :

> [TRADUCTION] « les problèmes globaux tels que la gestion des identités, les normes d'authentification et la protection de l'information dans le modèle hybride ne sont pas apparents. Une autre complication possible est qu'un nuage hybride peut changer au fil du temps avec l'adhésion et le départ des nuages qui le constituent ».[100]

Notons qu'il existe de multiples façons de configurer un modèle hybride et que la configuration la plus simple serait le « cloudbursting », consistant à répartir les charges entre les différents modèles selon les besoins[101].

À retenir…

Le modèle hybride implique généralement une combinaison de deux ou plusieurs modèles (privé, public et/ou communautaire), selon les besoins de l'organisation. Les avantages et les risques sont donc les mêmes en ce qui a trait à chaque type de modèle composant le système, mais on y ajoute une complexité découlant de l'architecture de sécurité particulière au système hybride. Il offre toutefois une grande flexibilité dans l'utilisation des ressources, surtout lorsque les besoins sont complexes et qu'ils impliquent une grande variété de données.

2) Les modèles de service

La notion de modèles de service renvoie aux types de ressources auxquelles un utilisateur du nuage peut avoir accès. Ainsi, les modèles de service les plus courants sont normalement regroupés sous trois catégories, à savoir : les logiciels sous forme de service (i), la plateforme sous forme de service (ii) et l'infrastructure sous forme de service (iii). Toutefois, notons que

[99] L. BADGER *et al.*, préc., note 18, p. 4-16.

[100] *Id.*, p. 4-15.

[101] *Id.*, p. 4-16.

cette liste n'est aucunement exhaustive et que divers autres modèles de services sont présentement utilisés dans l'industrie (iv). Comme pour les modèles de déploiement, notre définition de l'infonuagique passera donc par une analyse sommaire de ces différents modèles.

a) Les logiciels sous forme de service (SaaS)

i) Fonctionnement et caractéristiques

- *Fonctionnement*

Le modèle logiciel sous forme de service ou SaaS (pour *Software as a Service*), fait référence à l'utilisation d'un logiciel commercialisé en tant qu'application à distance, accessible comme un service, par le biais d'Internet[102]. Il peut appartenir, être délivré et être géré à distance par un ou plusieurs prestataires[103].

Le SaaS peut être déployé sur Internet et/ou derrière un pare-feu, sur un espace réseau local ou un ordinateur personnel[104]. Normalement, les logiciels sont prêts à être utilisés et sont mis à jour régulièrement, sans besoin d'interventions de la part de l'utilisateur. Tout comme l'ASP (Application Service Provider – ou fournisseur d'applications hébergées[105]) ou les applications à la demande[106], le SaaS s'inscrit dans la famille des logiciels hébergés. Le prestataire de SaaS peut soit héberger lui-même le logiciel sur ses propres serveurs ou le déployer sur une infrastructure appartenant à un tiers-prestataire[107].

Ce modèle conviendrait à « certaines catégories d'applications qui se doivent d'être globalement identiques pour tout le monde, la standardisation étant un des principes du cloud »[108]. En effet,

---

[102] Voir: JOURNAL DU NET, « SaaS : définition, offre et retours d'expérience », en ligne : < http://www.journaldunet.com/ solutions/intranet-extranet/saas/ >.

[103] GARTNER, « IT Glossary », en ligne : < http://www.gartner.com/it-glossary/software-as-a-service-saas/ >.

[104] S. SUBASHINI et V. KAVITHA, préc., note 23, 6.

[105] « Société qui offre en location, souvent en ligne, des progiciels ou des logiciels d'application avec tous les services connexes ». Voir OLF, préc., note 3.

[106] « Modèle de distribution en ligne de logiciels dans lequel un usager obtient la copie de l'un d'entre eux d'un hébergeur à qui il doit payer une somme d'argent pour son usage ». Voir OLF, préc., note 3.

[107] *Id.* p. 3.

[108] SYNTEC NUMÉRIQUE, préc., note 10, p. 6.

« [l]e terme SaaS évoque bien un service dans le sens où le fournisseur vend une fonction opérationnelle, et non des composants techniques requérant une compétence informatique »[109]. Ainsi, l'utilisateur n'a normalement pas besoin de gérer ou de contrôler l'infrastructure comme les serveurs, les systèmes opérationnels ou l'espace de stockage[110].

- *Services offerts*

L'accès aux services se fait à la demande par le biais d'applications logicielles, moyennant un tarif à l'heure, à l'utilisation, selon le nombre d'utilisateurs ou selon la quantité de données stockées[111]. Il s'agit du modèle infonuagique le plus utilisé, puisqu'il comprend notamment les boîtes de messagerie électronique, la gestion des relations clients, la planification des ressources, la gestion des documents, les réseaux sociaux et plusieurs applications offertes en ligne par Google et Amazon[112].

ii) Avantages et inconvénients

- *Avantages*

Avec le SaaS, le client n'a plus besoin de mettre en place et d'exploiter à l'interne l'infrastructure informatique sous-jacente au logiciel[113]. De même, il n'est plus nécessaire de gérer les processus de mise à jour d'applications ou d'installation de correctifs, ceux-ci relevant du prestataire SaaS[114]. Les SaaS facilitent ainsi le déploiement d'applications et permettent d'éviter les coûts et les complications liés à l'achat et à la maintenance d'un logiciel[115]. En effet, ils nécessitent très peu d'espace disque sur l'ordinateur pour le client, puisque les logiciels sont installés sur les serveurs et non sur les postes des utilisateurs. On élimine ainsi les problèmes de configuration ou

[109] *Id.*

[110] P. MELL et T. GRANCE, préc., note 8.

[111] L. BADGER *et al.*, préc., note 18, p. 5-1.

[112] *Id.*

[113] P. MELL et T. GRANCE, préc., note 8.

[114] L. BADGER *et al.*, préc., note 18, p. 5-4.

[115] *Id.* p. 5-5. Voir également « IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », (2011) *L'informaticien*, en ligne : < http://www.linformaticien.com/dossiers/id/20578/iaas-paas-et-saas-les-trois-grands-modeles-de-service-du-cloud.aspx >.

d'espace disque insuffisant[116]. D'autre part, comme la responsabilité de la gestion des plateformes est assumée par les prestataires[117], les utilisateurs ne sont généralement pas impliqués dans la gestion de l'infrastructure.

Pour le modèle SaaS public, la gestion des données par le prestataire est centralisée et la plupart des données vont résider sur les serveurs de celui-ci. Selon le NIST, l'accès à la demande libère les utilisateurs de la nécessité de transporter leurs données, ce qui réduit potentiellement les risques de perte et de vol[118].

Par ailleurs, l'efficacité d'utilisation des licences est grandement augmentée avec l'utilisation du modèle SaaS. En effet, le nombre de licences est ajustable « à la hausse comme à la baisse alors que dans le mode traditionnel, une licence achetée l'est à titre définitif »[119]. Les utilisateurs peuvent utiliser une seule licence sur plusieurs ordinateurs à différents moments au lieu de se procurer des licences supplémentaires pour les ordinateurs additionnels. En outre, la gestion des licences par le prestataire ne requiert pas de protéger la propriété intellectuelle, puisque les logiciels fonctionnent à partir de l'infrastructure du prestataire. Leur utilisation peut donc être directement mesurée et facturée[120].

Le modèle SaaS public et externe peut être utilisé sans coût d'acquisition d'équipement, mais possiblement avec un coût d'usage récurrent[121]. Mentionnons qu'une analyse précise de tous les coûts envisageables devrait être effectuée avant d'utiliser le SaaS, puisque la variation dans l'utilisation et l'augmentation éventuelle du prix des licences pourraient avoir une incidence sur la pertinence de recourir à ce type de service[122].

---

[116] L. BADGER *et al.*, préc., note 18, p. 5-4.

[117] L. BADGER *et al.*, préc., note 18, p. 5-4.

[118] *Id.*, p. 5-4.

[119] « IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », préc., note 115.

[120] L. BADGER *et al.*, préc., note 18, p. 5-4.

[121] *Id.*, p. 5-5.

[122] *Id.*

- Inconvénients

Pour que le modèle SaaS puisse être utilisé, les données doivent être collectées chez le client et être transférées via un réseau. Ceci implique que le réseau soit équipé de technologies de cryptage efficaces afin de contrer les possibilités d'intrusion et d'assurer un transfert sécuritaire des données[123]. En raison, notamment, des applications multiples et des bases de données, la complexité des systèmes infonuagiques engendre des risques pour l'intégrité des données. Comme dans tous les autres modèles, il devra être tenu compte de ce risque pour mettre en œuvre le SaaS :

> « In order to maintain data integrity in a distributed system, transactions across multiple data sources need to be handled correctly in a fail safe manner. This can be done using a central global transaction manager. Each application in the distributed system should be able to participate in the global transaction via a resource manager ».[124]

Nous avons déjà abordé la question des risques liés aux architectures partagées des systèmes infonuagiques. Dans le cas du SaaS, des utilisateurs multiples peuvent stocker leurs données dans diverses applications offertes par un même prestataire. Ceci engendre un risque que les données de clients distincts résident de manière conjointe au même emplacement. De la sorte, des intrusions peuvent se produire, en piratant l'application ou en injectant des lignes de codes dans le système[125]. Le modèle SaaS doit donc assurer une frontière définie entre les données de chaque utilisateur, assurée non seulement au niveau physique, mais également au niveau de l'application[126]. Ainsi, le service devrait être apte à séparer les données des différents utilisateurs.

Le plus souvent, le logiciel SaaS est hébergé et exploité à l'extérieur du pare-feu de l'organisation cliente. Les organisations doivent donc veiller à gérer les renseignements de

---

[123] Voir *id*., p. 5-5, 5-6. Les types de vulnérabilités relatives à la sécurité des données dans le modèle SaaS peuvent prendre plusieurs formes : « Cross-site scripting [XSS], Access control weaknesses, OS and SQL injection flaws, Cross-site request forgery [CSRF], Cookie manipulation, Hidden field manipulation, Insecure storage, Insecure configuration, Network penetration and packet analysis, Session management weaknesses, Insecure SSL trust configuration ». Voir S. SUBASHINI et V. KAVITHA, préc., note 23, 4.

[124] S. SUBASHINI et V. KAVITHA, préc., note 23, 5.

[125] L. BADGER *et al.*, préc., note 18.

[126] *Id.*

manière à ne pas oublier de faire ajouter ou supprimer certaines données du système SaaS, selon le traitement requis. Par exemple, les ressources humaines d'une organisation devraient faire détruire systématiquement les données des employés qui quittent leur emploi. Ceci implique un système de gestion des technologies de l'information efficace et, considérant le nombre d'employés embauchés dans certaines organisations, nous supposons que plusieurs effectifs seront requis pour assurer la destruction et l'archivage de certaines données.

Comme nous le verrons plus loin, même si les navigateurs chiffrent leurs communications avec les prestataires de services infonuagiques, un risque de divulgation des données demeure possible selon le NIST. En effet, « l'approche SaaS augmente aussi le risque que l'accès à une application compromette les données d'un client dans l'éventualité où celui-ci consulte un site Web malicieux et le navigateur se retrouve contaminé »[127].

D'autre part, la disponibilité des applications dépendra en grande partie de la fiabilité et de la disponibilité continue du réseau, tel que nous l'avons vu pour le modèle de déploiement public. Dans le scénario SaaS privé externe ou communautaire, un niveau raisonnable de sécurité et de fiabilité du réseau pourra être atteint en utilisant des liens de communication protégés. Évidemment, une telle infrastructure nécessitera d'importants investissements[128].

Les prestataires d'applications SaaS peuvent reproduire plusieurs copies de sauvegarde des données qui leur sont confiées et les conserver à différents endroits dans le monde, afin d'en assurer une meilleure disponibilité. La possibilité de répliquer les données peut constituer un avantage, mais nous sommes d'avis qu'elle constitue également un risque important, puisqu'une plus grande disponibilité des données augmente les risques de divulgation et d'accès non autorisé[129]. Qui plus est, un tel modèle d'affaire implique, pour l'utilisateur, une certaine perte de contrôle sur ses données[130], sans compter le fait que, comme nous le verrons dans la seconde partie de la présente étude, la multiplication des lieux où pourraient être situées les données d'un

[127] *Id*.

[128] *Id*., p. 5-6.

[129] Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Yvon Blais, 2010.

[130] S. SUBASHINI et V. KAVITHA, préc., note 23, 4.

utilisateur peut avoir des implications juridiques importantes. Un modèle SaaS sécuritaire devrait donc permettre d'identifier l'emplacement des données d'un utilisateur et d'en informer ce dernier[131].

En définitive, les modèles SaaS doivent être suffisamment flexibles pour incorporer les différentes politiques de sécurité des clients. Le prestataire du SaaS devrait aussi être capable de fournir des barrières organisationnelles à l'intérieur de son système, en raison du déploiement des différents processus d'affaires par les organisations dans un même environnement infonuagique[132].

À retenir…

Le SaaS est un logiciel commercialisé en tant qu'application à distance, accessible comme un service, par le biais d'Internet et du Web. L'organisation cliente n'a donc plus besoin d'exploiter à l'interne l'infrastructure informatique sous-jacente au logiciel.

b) La plateforme sous forme de service (PaaS)

i) Fonctionnement et caractéristiques

- *Fonctionnement*

Le modèle plateforme sous forme de service ou PaaS (pour *Platform as a Service*), aussi appelé « cloud applicatif »[133], permet un accès aux données via une « plateforme informatique (serveur, dispositif de stockage ou ordinateur) reliée à Internet et hébergée par un opérateur »[134]. Ce type de plateforme « permet […] aux développeurs de créer des applications exécutables à partir du

[131] *Id.,* p. 5.

[132] *Id.*

[133] « IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », préc., note 115.

[134] P. JOSET, préc., note 12.

nuage ou d'utiliser les services que fournit le nuage »[135]. Ces plateformes peuvent également « être mises à la disposition des entreprises qui désirent héberger leurs applications »[136].

- Services offerts

Selon le NIST, le service qui est fourni au client serait « la capacité de déployer des applications, qu'il a créé ou acquis, sur l'infrastructure infonuagique en utilisant des langages et outils de programmation supportés par le fournisseur »[137]. Ainsi, le client ne gère et ne contrôle pas l'infrastructure infonuagique sous-jacente incluant le réseau, les serveurs, les systèmes d'opération ou le stockage, mais il garde un certain contrôle sur le déploiement des applications et peut-être même sur les configurations de l'environnement d'hébergement des applications[138].

En autres mots, le PaaS fournit une boîte à outils aux utilisateurs pour le développement, le déploiement et la gestion d'applications logicielles structurées de manière à supporter une grande quantité d'utilisateurs et pour traiter une quantité importante de données, en étant accessible de n'importe où via Internet[139]. Les services PaaS qui sont offerts aux clients incluent le développement de plateformes et la gestion de bases de données, la gestion opérationnelle du système, le bureau virtuel et la livraison de services Web[140]. Le site Facebook est l'un des exemples de PaaS les plus couramment utilisés, puisqu'il permet aux développeurs de créer des applications spécifiques en utilisant une interface de programmation propriétaire et de rendre cette application disponible à n'importe quel utilisateur Facebook[141].

---

[135] *Id.*

[136] *Id.*

[137] P. MELL et T. GRANCE, préc., note 8 [notre traduction].

[138] *Id.*

[139] L. BADGER *et al.*, préc., note 18, p. 6-1.

[140] *Id.*, p. 5-10.

[141] Voir Irene BODLE, « SaaS Agreements – SaaS, PaaS, IaaS – Is There a Difference? », (2012) *Bodle Law*, en ligne : < http://www.bodlelaw.com/saas/saas-agreements-saas-paas-iaas-is-there-a-difference >.

ii) Avantages et inconvénients

- *Avantages*

Le modèle PaaS comporterait les mêmes avantages que le SaaS en termes de gestion des applications et des infrastructures, de centralisation des données et d'économie de coûts[142]. Cependant, il serait doté d'un avantage supplémentaire au niveau de « l'extensibilité des applications »[143]. Le PaaS serait par ailleurs le plus avantageux pour les techniciens, car il permettrait de « réaliser des projets urgents ou qui nécessiteraient des ressources informatiques à la demande »[144].

- *Inconvénients*

Le PaaS présente plusieurs des inconvénients déjà cités pour le modèle SaaS, dont les risques liés au fonctionnement des navigateurs et à la dépendance du réseau Internet. Il comporte toutefois d'autres inconvénients qui lui sont spécifiques. En général, la migration d'applications existantes vers le modèle PaaS est compliquée, car les applications doivent être réécrites selon le type de plateforme visé. Or, « les langages de programmation sont parfois propriétaires, comme Apex sur Force.com, et seuls les modules logiciels […] disponibles sur la plate-forme sont utilisables »[145].

De plus, un développeur d'applications PaaS devra gérer une multitude de risques de sécurité. En effet, le PaaS accède au réseau de manière intrinsèque, doit utiliser la cryptographie et interagir avec les particularités des navigateurs communs qui offrent un *output* aux consommateurs[146].

En pratique, ce type de modèle poserait surtout des contraintes techniques. Selon certains, la réussite d'un tel projet dépendrait ainsi de deux facteurs : « les compétences en développement

---

[142] L. BADGER *et al.*, préc., note 18, p. 6-3.

[143] *Id.*, p. 6-4.

[144] « L'Approche Platform as a Service (Paas) », (2011) *01Business*, en ligne : < http://pro.01net.com/editorial/520437/lapproche-platform-as-a-service-%28paas%29/ >.

[145] *Id.*

[146] L. BADGER *et al.*, préc., note 18, p. 6-5.

dont dispose l'entreprise cliente et le type d'applications qu'elle souhaite mettre en PaaS, les deux étant intimement liés »[147].

À retenir…

Le PaaS fournit une boîte à outils aux utilisateurs pour le développement, le déploiement et la gestion d'applications logicielles structurées de manière à supporter une grande quantité d'utilisateurs et pour traiter une quantité importante de données, en étant accessible de n'importe où via Internet.

c) L'infrastructure sous forme de service (IaaS)

i) Fonctionnement et caractéristiques

- *Fonctionnement*

L'infrastructure sous forme de service ou IaaS (pour *Infrastructure as a service*), aussi appelée « cloud d'infrastructure »[148], est un modèle où l'infrastructure, le réseau et le dispositif de stockage sont offerts par un prestataire. L'infrastructure traditionnellement constituée de serveurs, de postes de travail et d'équipement réseau est désormais mise à la disposition du client par le biais d'Internet et peut être améliorée ou diminuée en fonction des besoins[149]. Le client ne gère pas l'infrastructure infonuagique sous-jacente, mais il exerce un contrôle sur les systèmes d'opération, le stockage, les applications déployées et possiblement un contrôle limité de certains composants de réseaux (par exemple, pare-feu hôtes)[150]. Les prestataires de ce type de service facturent habituellement à l'utilisation, et la quantité de ressources utilisées et le coût reflètent habituellement le niveau d'activité de l'utilisateur[151].

- *Services offerts*

Les services fournis par le IaaS comprennent le réseautage, le stockage, les réseaux de distribution de contenu pour améliorer la performance et/ou le coût de servir les clients Web et un

[147] « L'Approche Platform as a Service (Paas) », préc., note 144.

[148] « IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », préc., note 115.

[149] M. TREMBLAY, préc., note 15.

[150] P. MELL et T. GRANCE, préc., note 8.

[151] INSTITUT CANADIEN DES COMPTABLES AGRÉÉS, préc., note 11.

service de sauvegarde et de récupération[152]. « [U]ne entreprise pourra par exemple louer des serveurs Linux, Windows ou autres systèmes, qui tourneront en fait dans une machine virtuelle chez le fournisseur de l'IaaS »[153].

ii) Avantages et inconvénients

- *Avantages*

Le IaaS est un modèle qui « libère l'entreprise de la nécessité de posséder (gérer, maintenir et contrôler, etc.) ses propres serveurs et autres infrastructures de traitement de données. Il suffira d'un ordinateur ou un portable connecté à Internet pour lui garantir sa fonctionnalité commerciale. [...] La réduction des coûts d'acquisition, de maintenance et de recyclage des équipements est importante pour les entreprises. Le risque de pannes et d'interruption d'activité est aussi minimisé, vu la très haute fiabilité de ce genre de services en ligne »[154].

En outre, le modèle IaaS offrirait une flexibilité et une efficacité de la location du matériel informatique. En fournissant les fonctionnalités d'un accès au « hardware », les modèles IaaS publics et externes offrent ainsi la possibilité de louer rapidement et ponctuellement un grand nombre de machines virtuelles ou autres ressources du nuage[155]. Ceci donne au client la possibilité de rapidement mettre en place de vastes réseaux de machines virtuelles qui exécutent des logiciels choisis pour résoudre d'importants problèmes, sans encourir les frais d'achat et d'entretien du matériel nécessaire[156].

Selon le NIST, les trois différentes formes d'accès aux ressources du IaaS permettent un contrôle quasi-total sur les outils informatiques. En premier lieu, un utilisateur émet des commandes administratives au prestataire du nuage, comme des requêtes pour faire fonctionner des systèmes virtuels ou pour sauvegarder les données sur les serveurs du nuage. En second lieu, un utilisateur

---

[152] L. BADGER *et al.*, préc., note 18, p. 6-1.

[153] SYNTEC NUMÉRIQUE, préc., note 10, p. 6.

[154] « Cloud computing le concept », *Cloud Computing*, en ligne : < http://cloudcomputing.fr/laas-paas-saas.php >.

[155] L. BADGER *et al.*, préc., note 18, p. 7-6.

[156] *Id.*

ayant des droits d'administrateur pour les machines virtuelles identifiées émet des commandes administratives auxdites machines virtuelles. En dernier lieu, n'importe quel utilisateur, et même un utilisateur anonyme avec accès au réseau public, interagit avec les machines virtuelles en utilisant les services fonctionnant en réseau sur lesdites machines virtuelles[157].

Certains auteurs sont d'avis que le IaaS offre ainsi « la plus grande marge de manœuvre, la plus grande flexibilité et le plus grand contrôle en permettant de migrer tout type d'application métier existante dans le Cloud, et de déplacer tout type de serveur afin de réduire ses coûts »[158]. Par ailleurs, un haut niveau de compatibilité peut être maintenu entre les applications d'origine et les charges de travail, ce qui permet aux utilisateurs d'installer et de faire fonctionner les systèmes librement[159].

- Inconvénients

De la même manière que les modèles SaaS et PaaS, l'utilisation du modèle IaaS dépendra de la fiabilité du réseau et du bon fonctionnement des navigateurs[160]. De plus, en permettant aux clients de faire fonctionner les logiciels hérités dans l'infrastructure du prestataire, le modèle IaaS expose les clients aux menaces de sécurité de ces logiciels hérités[161].

En outre, la responsabilité de gérer les identités pour accéder aux services infonuagiques du prestataire incombera au client. Généralement, le navigateur de l'utilisateur utilisera la cryptographie à clé publique pour sécuriser les communications entre celui-ci et le prestataire, mais il reviendra au client de s'assurer que les utilisateurs sont valablement authentifiés[162].

---

[157] *Id.*

[158] « IaaS, PaaS et SaaS avantages et inconvénients », (2012) *Yes We Cloud*, en ligne : < http://www.yeswecloud.fr/cloud/iaas-paas-et-saas-avantages-et-inconvenients-629.html >.

[159] *Id.*

[160] L. BADGER *et al.*, préc., note 18, p. 7-6.

[161] *Id.*, p. 7-7.

[162] *Id.*

Afin de prévenir des interactions non désirées entre les clients distincts, le réseau du IaaS doit pouvoir empêcher qu'un utilisateur accède aux paquets de données[163] envoyés dans le système par d'autres utilisateurs. Le prestataire doit de plus s'assurer que ceux-ci disposent d'une bande passante suffisante[164]. De plus, certaines politiques de destruction des données peuvent ne pas être compatibles avec la performance lorsque les utilisateurs du service changent. Les pratiques de sauvegarde et de copie des données peuvent aussi compliquer la destruction de celles-ci[165].

Les systèmes IaaS permettent aux clients de créer et même possiblement de conserver de nombreuses machines virtuelles dans différents états[166]. Qui plus est, les mesures de sécurité associées à une machine virtuelle inactive peuvent facilement devenir obsolètes[167]. En effet, même si un prestataire pouvait, en principe, mettre à jour les machines virtuelles inactives au nom des clients, les mécanismes de cette mise à jour sont complexes et le maintien des mises à jour de sécurité est généralement de la responsabilité de l'utilisateur[168].

À retenir…

L'IaaS libère l'organisme client de la nécessité de posséder et d'entretenir ses propres serveurs et autres infrastructures de traitement de données. Si ce modèle présente des avantages évidents quant aux frais de maintenance des équipements, il implique par ailleurs une dépendance accrue au prestataire.

[163] « Ensemble de bits et d'éléments numériques de service constituant un message ou une partie de message, organisé selon une disposition déterminée par le procédé de transmission et acheminé comme un tout ». Voir OLF, préc., note 3.

[164] L. BADGER *et al.*, préc., note 18, p. 7-6.

[165] *Id.*, p. 7-8: [TRADUCTION] « Quand un utilisateur libère une ressource, le fournisseur doit s'assurer que le prochain utilisateur de la ressource n'ait pas accès aux données provenant des utilisateurs précédents. Des politiques d'effacement de données efficaces (par exemple, l'écrasement multiple de blocs de disque) prennent beaucoup de temps à mettre en œuvre et peuvent affecter la performance lors du changement d'utilisateurs. La duplication et la sauvegarde des données compliquent également les pratiques de suppression de données ».

[166] Par exemple, en cours, suspendues et fermées. Voir *id.*

[167] *Id.*, p. 7-7.

[168] *Id.*

d) Autres types de modèles disponibles

Depuis quelques années, de nouveaux modèles de services infonuagiques ont émergé. Bien qu'ils puissent disposer de leurs propres spécificités, leur fonctionnement se recoupe avec les trois modèles principaux expliqués ci-haut. Vous trouverez dans le lexique disponible en annexe une description de certains modèles présentement disponibles, soit le « Network as a service », le « Business Process as a service » et le « Desktop as a service ». Notons que d'autres options sont aussi actuellement possibles, comme le « Storage as a service », le « Workplace as a service » et le « Data as a Service ». L'infonuagique étant une technologie en constante évolution, nous prévoyons que d'autres modèles seront développés dans l'avenir et offriront de multiples possibilités de service.

Pour conclure, nous pouvons donc résumer la présente section de notre étude en indiquant que la notion d'infonuagique englobe une panoplie de services découlant de différents modèles de déploiement et de service. Si cela implique un nombre quasi-infini de définitions et d'exemples possibles, tous ces exemples incorporent une externalisation de services informatiques qui, si elle peut permettre certains gains financiers et en productivité, peut entrainer certains risques liés à une perte de contrôle sur les données de l'organisation, ainsi que sur la sécurité de l'information et des infrastructures. Ainsi, pour un gouvernement, tout recours à l'infonuagique devra établir un équilibre entre ces deux considérations. Comme nous le verrons maintenant, c'est ce qu'ont fait les quelques états ayant incorporé certaines solutions infonuagiques dans leurs politiques de gestion de l'information.

B. Les exemples d'utilisation de solutions d'infonuagique par différents États

Afin de mieux comprendre les incidences de l'adoption d'une éventuelle stratégie infonuagique gouvernementale québécoise, il devient utile d'identifier les embûches qu'ont dû affronter les différents états ayant déjà adopté une telle politique, ou dont la réflexion est plus avancée que celle du gouvernement du Québec. Évidemment, l'exhaustivité demandée par un tel exercice dépasserait le cadre de la présente étude, d'autant plus que le *Laboratoire d'étude sur les politiques publiques et la mondialisation* a déjà procédé à une analyse semblable. Nous avons

donc opté pour un échantillonnage d'exemples canadiens (1) et internationaux (2) qui nous sont apparus particulièrement instructifs vu la portée du mandat nous ayant été confié.

1) Les exemples canadiens

Au niveau national, nous avons opté d'analyser la position du gouvernement canadien (a) puisque celle-ci aura immanquablement des incidences sur toute politique provinciale. En effet, comme nous le verrons, certains des choix politiques du gouvernement du Canada auront des incidences sur la possibilité, pour une province, d'héberger des données à l'extérieur de ses frontières. Quant aux autres provinces canadiennes, une analyse initiale nous a permis d'identifier la Colombie-Britannique (b) et la Saskatchewan (c) comme étant les deux provinces où la réflexion étatique liée à l'adoption d'une stratégie infonuagique gouvernementale était la plus avancée ou, tout au moins, la mieux documentée. Ce sont donc ces trois juridictions qui feront l'objet de la présente section de notre étude.

a) Le gouvernement du Canada

Notre analyse de la position du gouvernement canadien quant à l'infonuagique se base notamment sur les principes évoqués par le Commissariat à la protection de la vie privée du Canada (ci-après : le « CPVPC ») dans différents rapports, dont le « Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et l'infonuagique »[169] (ci après : le « Rapport de 2010 »), le rapport intitulé « Visez les nuages : Questions liées à la protection de la vie privée dans le contexte de l'informatique dans les nuages »[170], résumant les risques pour la vie privée associés à l'utilisation de l'infonuagique et les « Lignes directrices pour le traitement transfrontalier des données » (ci-après : les « Lignes directrices »), lesquelles expliquent notamment de quelle manière la *Loi sur la protection des renseignements personnels et les* documents électroniques[171] (ci-après : la « *LPRPDÉ* ») s'applique aux transferts de renseignements personnels à des tiers, que ceux-ci se trouvent au Canada ou à l'étranger.

---

[169] CPVPC, préc., note 25.

[170] CPVPC, préc., note 9.

[171] LC 2000, c 5.

Nous discuterons également du rapport de conclusions d'enquête sur la *LPRPDÉ* n° 2005-313 intitulé « Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA Patriot Act* », afin d'en dégager les recommandations relatives à l'externalisation des renseignements personnels et à l'infonuagique.

i) Contraintes juridiques

La mise en place d'un système infonuagique de traitement de données sera soumis, selon l'entité visée, soit à la *LPRPDÉ*, soit à la *Loi sur la protection des renseignements personnels*[172] (ci-après : la « *LPRP* »). Rappelons que la *LPRPDÉ* régit la façon dont les organisations du secteur privé peuvent recueillir, utiliser et communiquer des renseignements personnels dans le cadre de leurs activités commerciales et qu'elle s'applique également aux entreprises fédérales pour ce qui est des renseignements personnels des employés[173]. De son côté, la *LPRP* « a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent »[174]. Ainsi, si le gouvernement canadien décidait de mettre en place un système infonuagique de traitement des données, c'est la *LPRP* qui trouverait application[175].

Ni la *LPRPDÉ*, ni la *LPRP* n'interdisent le recours à l'infonuagique, même lorsqu'un tel choix implique le transfert de données personnelles à l'étranger par les organisations canadiennes aux fins de traitement[176]. En fait, à l'exception de la Colombie-Britannique et de la Nouvelle-

---

[172] LRC 1985, c. P-21.

[173] CPVPC, « La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) », (2013), en ligne : < http://www.priv.gc.ca/leg_c/leg_c_p_f.asp >.

[174] *LPRP*, art. 2.

[175] CPVPC, préc., note 9.

[176] CPVPC, « Traitement transfrontalier des données personnelles : Lignes directrices », (2009), en ligne : < https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.pdf >; Kris KLEIN, « Clarification de l'application du droit canadien de la protection des renseignements personnels au transfert transfrontalier de ces renseignements du Canada vers les États-Unis », (2008) *Industrie Canada*, en ligne : < http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Clarification%20de%20l%E2%80%99application%20du%20droit%20canadien%20de%20la%20protection%20des%20renseignements%20personnels.pdf/$file/Clarification%20de%20l%E2%80%99application%20du%20droit%20canadien%20de%20la%20protection%20des%20renseignements%20personnels.pdf >, p. 12.

Écosse[177] qui disposent de règles spécifiques à cet égard, les lois en vigueur dans le reste du pays n'interdisent pas le traitement transfrontalier des données personnelles. Ainsi, toute organisation canadienne du secteur privé ou du secteur public peut en principe transférer des données personnelles à l'étranger par le biais de l'infonuagique[178], peu importe le modèle choisi.

Dans son Rapport de 2010[179], le CPVPC souligne que le détournement d'usage des renseignements personnels est une préoccupation importante. En effet, étant donné le faible coût de conservation des données, « les organisations ne sont pas enclines à s'en débarrasser, mais plutôt encouragées à les utiliser à d'autres fins »[180]. D'ailleurs, l'utilisation de l'infonuagique par les consommateurs semble faire l'objet d'inquiétudes plus grandes, découlant du faible contrôle qu'ils exercent sur leurs données et « où la transparence et le consentement pourraient être à risque »[181]. Le rapport poursuit en précisant que : « [c]ela peut aussi être problématique pour les très petites entreprises qui n'ont pas la capacité d'exercer la diligence raisonnable nécessaire avant de s'engager auprès d'un fournisseur de services infonuagiques »[182]. Le CPVPC est par ailleurs d'avis qu'un grand nombre de personnes « ne comprennent pas ou ont une compréhension très partielle de l'utilisation qui peut être faite de leurs renseignements personnels »[183].

Le CPVPC reconnaît qu'Internet ne facilite pas l'accès aux données par leurs titulaires et que la correction de celles-ci peut être complexe. Il précise que « les technologies, les modèles opérationnels et le nombre important d'intervenants font qu'il est très difficile pour les personnes de découvrir les renseignements détenus à leur sujet par les organisations et de corriger toute

---

[177] Comme nous le verrons plus loin, la Colombie-Britannique a adopté le *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165, visant à interdire le transfert de données aux États-Unis, sauf si un consentement à cet effet est obtenu. De la même manière, la Nouvelle-Écosse a adopté le *Personal Information International Disclosure Protection Act*, SNS 2006, c. 3. Voir K. KLEIN, préc., note 176, p. 14.

[178] *Id.*

[179] Préc., note 25.

[180] CPVPC, préc., note 25, p. 51.

[181] *Id.,* p. 52.

[182] *Id.*

[183] *Id.,* p. 54. Voir également : CPVPC, préc., note 9.

erreur factuelle »[184]. Cette problématique concernerait plus particulièrement la sécurité de l'information et la gestion des identités et de la réputation[185]. De plus, si plusieurs entreprises ou organisations utilisaient une infrastructure infonuagique communautaire, il pourrait y avoir un risque de confusion des demandes d'accès auprès du prestataire de services. En effet, celui-ci pourrait accidentellement recueillir l'information des autres entreprises et en divulguer le contenu. D'autre part, « la distance qui existe entre les données et leur propriétaire dans l'environnement de l'informatique dans les nuages accroît la possibilité non seulement que les intéressés ne soient pas conscients qu'il existe un accès légal à leurs données, mais que le fournisseur de services lui-même n'en soit pas conscient »[186].

Selon Kris Klein[187], il existe une croyance erronée à l'effet que les lois canadiennes sur la protection des renseignements personnels « obligent les organisations canadiennes à protéger les renseignements personnels contre l'accès légal d'un gouvernement étranger à ces renseignements »[188]. Il mentionne que la majorité des pays, dont le Canada, ont adopté des lois qui permettent aux institutions gouvernementales « d'avoir accès aux renseignements personnels de leur administration à des fins de sécurité nationale et d'application de la loi »[189]. Il ajoute que :

> « La Commissaire à la protection de la vie privée l'a reconnu lorsqu'elle a expliqué qu'il est conforme aux lois en vigueur aux États-Unis, au Canada et ailleurs de permettre aux gouvernements de recueillir des renseignements personnels dans le cadre d'activités relatives au renseignement : les gouvernements de par le monde exercent depuis longtemps le droit d'accéder aux renseignements détenus par les organisations se trouvant sur leur territoire. Plusieurs lois canadiennes permettent aussi aux organismes policiers et organismes de sécurité ainsi qu'aux ministères fédéraux généralement d'obtenir l'accès aux renseignements personnels détenus au Canada. »[190]

---

[184] CPVPC, préc., note 25, p. 52.

[185] *Id.*

[186] CPVPC, préc., note 9.

[187] K. KLEIN, préc., note 176.

[188] *Id.,* p. 4.

[189] *Id.*

[190] *Id.*

En effet, comme l'a souligné la Commissaire : « au Canada, de tels renseignements peuvent être obtenus en vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, de la *Loi sur le ministère de la Citoyenneté et de l'Immigration* et de la *Loi sur le Service canadien du renseignement de sécurité* »[191].

En outre, comme nous le verrons plus en détails dans la seconde partie de la présente étude, les procédures de surveillance augmentées par le *USA PATRIOT Act*[192] aux États-Unis permettraient au gouvernement américain d'accéder à nos données lorsqu'elles sont hébergées dans le nuage. En effet, l'article 215 du *USA PATRIOT Act*, permet au Federal Bureau of Investigation (« FBI ») d'avoir accès à des dossiers détenus aux États-Unis, « en demandant une ordonnance de la Foreign Intelligence Surveillance Act Court of Review »[193]. Une organisation faisant l'objet d'une telle ordonnance ne peut révéler qu'elle a fourni des renseignements au FBI suite à cette ordonnance[194]. Tel que le confirme un rapport de l'Université d'Amsterdam, les États-Unis auraient ainsi accès aux données contenues dans les systèmes appartenant à des entreprises américaines :

> « The U.S. government has ample possibilities to request data from foreign (in this case Dutch) users of the cloud. The most striking example in this regard is the specific provision (50 USC § 1881a) introduced in 2008 for the acquisition of data of non-U.S. persons outside the United States, given the far-reaching powers it grants to retrieve information on a large scale, including access to complete data sets. U.S. authorities also have powers to request information from cloud providers in the context of criminal investigations. Jurisdiction under U.S. law is a necessary precondition, which is effectuated when cloud providers are based in the United States or if they conduct continuous and

[191] *Id.*, p. 4.

[192] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, PUBLIC LAW 107–56—OCT. 26, 2001.

[193] CPVPC, « Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA Patriot Act* », Résumé de conclusions d'enquête en vertu de la *LPRPDE* n° 2005-313.

[194] *Id.*

> systematic business in the United States. It is a misconception that U.S. jurisdiction applies only if the data are physically located on U.S. territory ».[195]

La « juridiction extra-territoriale »[196] de l'encadrement légal américain implique que tous les prestataires de services infonuagiques opérant n'importe où dans le monde doivent se conformer à des requêtes sur les données qui tombent sous l'application des lois américaines. Celles-ci s'appliquent aux prestataires de services dès lors que ceux-ci exercent des activités aux États-Unis. Les données ne doivent donc pas être nécessairement stockées sur des serveurs physiquement présents sur le territoire américain pour que le gouvernement puisse y accéder. Ceci implique que les données de Canadiens pourront être accessibles par le gouvernement américain dès qu'elles seront stockées dans l'infonuagique d'une entreprise américaine.

Notons que les organisations canadiennes peuvent être sujettes à des ordonnances équivalentes à celles du *USA PATRIOT Act*, les obligeant à communiquer aux autorités canadiennes des renseignements personnels détenus au Canada[197]. En effet, la *LPRPDÉ* a été modifiée « de façon à permettre à des organisations de recueillir et d'utiliser des renseignements personnels sans consentement aux fins d'une communication de ces renseignements à des institutions gouvernementales si ces renseignements ont trait à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales »[198].

Par ailleurs, cette pluralité d'emplacements disponibles pour le traitement et le stockage de l'information rend l'infonuagique particulièrement concernée par les problèmes de compétences[199]. D'ailleurs, « [l]a prépondérance du modèle d'informatique dans les nuages pourrait même remettre en question la notion de "propriété" des données, sur laquelle repose une bonne partie du système de protection des données, ce qui conduirait plutôt à des analyses

---

[195] Joris VAN HOBOKEN, Axel ANRBAK et Nico VAN EIJK, « Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act », (2012) *SSRN*, en ligne : < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534 >.

[196] *Id.*

[197] CPVPC, préc., note 93.

[198] CPVPC, préc., note 9.

[199] *Id.*

fondées sur l'authentification des données »[200]. Ainsi, « la création de nouveaux flux de données pourrait susciter des inquiétudes quant à leur propriété »[201]. En effet, « [b]ien que la propriété des données confiées à une infrastructure d'informatique dans les nuages aux fins de stockage semble assez explicite, la propriété des données téléchargées vers une infrastructure d'informatique dans les nuages risque d'être moins certaine »[202]. Enfin, il est tout à fait possible que les utilisateurs ne soient pas informés de l'existence de « données secondaires générées par les interactions avec une infrastructure d'informatique dans les nuages »[203].

ii) Solution retenue

Selon les Lignes directrices, « les organisations doivent aviser les consommateurs de façon claire et compréhensible que leurs renseignements personnels pourraient être traités dans un pays étranger, et que les organismes d'application de la loi et de sécurité nationale de ce pays pourraient y accéder »[204]. En outre, les organisations « sont tenues de protéger les renseignements personnels qui se trouvent entre les mains des tiers qui les traitent. Le moyen principal d'assurer cette protection est par voie contractuelle »[205]. Le CPVPC est ainsi d'avis qu'une évaluation des risques pour l'intégrité, la sécurité et la confidentialité des renseignements personnels de leurs clients « au moment ou à la suite du transfert à un tiers fournisseur de services exerçant des activités à l'extérieur du Canada »[206] doit être effectuée.

En vertu de la *LPRPDÉ*, les données ne peuvent être conservées que pour la durée nécessaire aux fins déterminées[207]. Dans son Rapport sur les consultations de 2010, le CPVPC indique que, « compte tenu du modèle de responsabilité décrit dans la loi, on s'attend à ce que les organisations qui s'engagent par contrat avec un fournisseur de services infonuagiques imposent

[200] *Id.*

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] CPVPC, préc., note 176, p. 8.

[205] *Id.*

[206] *Id.*

[207] CPVPC, préc., note 25, p. 52.

certaines restrictions et mènent des vérifications »[208]. Il suggère également que des normes de sécurité pour l'utilisation des services infonuagiques soient établies par le gouvernement[209] et que le signalement des incidents soit rendu obligatoire en vertu de la *LPRPDÉ*[210], soulignant que :

> « les personnes ont de la difficulté à se plaindre de pratiques qu'elles ne connaissent pas du tout. Bon nombre de personnes ne savent même pas que leurs renseignements personnels se trouvent dans une infrastructure infonuagique, et les incidents ont souvent pour effet de le leur faire savoir. Un résultat très positif du signalement obligatoire des atteintes à la protection de la vie privée est probablement la transparence. Les participants ont laissé entendre que, si cela était rendu obligatoire, les organes de réglementation auraient une meilleure connaissance de la situation et pourraient offrir une orientation afin d'améliorer les pratiques ».[211]

En outre, le Rapport de conclusions d'enquête 2005-313[212] du CPVPC souligne que la « [l]oi ne peut empêcher les autorités américaines d'avoir accès légalement aux renseignements personnels de Canadiennes et de Canadiens que possèdent des organisations au Canada ou aux États-Unis, pas plus qu'elle ne peut obliger les sociétés canadiennes à mettre fin à l'impartition de services à des fournisseurs établis à l'étranger »[213]. Cependant, les organisations doivent faire « preuve de transparence au sujet de leurs méthodes de traitement des renseignements personnels et que, grâce à des moyens contractuels, elles protègent dans toute la mesure du possible les renseignements personnels de clients qui sont entre les mains de tiers fournisseurs de services établis à l'étranger »[214].

b) La Colombie-Britannique

Le gouvernement de la Colombie Britannique envisage de plus en plus de recourir aux services infonuagiques afin de tirer parti de ses avantages, soit les économies et les fonctionnalités

---

[208] *Id.*

[209] *Id.,* p. 50.

[210] *Id.*, p. 54.

[211] *Id.,* p. 50.

[212] CPVPC, préc., note 193.

[213] *Id.*

[214] *Id.*

offertes[215]. En 2012, le Bureau du Commissaire à l'information et à la vie privée de la Colombie-Britannique (ci-après : le « CIVPCB ») a publié un document intitulé « Cloud Computing Guidelines for Public Bodies »[216], lequel porte sur les incidences de la *Freedom of Information and Protection of Privacy Act* (« FIPPA » ou « FOIPPA »)[217] sur l'utilisation de l'infonuagique par les institutions gouvernementales[218]. Le rapport décrit l'infonuagique comme suit :

> « The rise of "cloud computing" – the practice of using the Internet to process, manage and store data on remote network services – now permits individuals to perform traditionally private activities on the Internet. This computing trend is fuelling a mass migration of information, once stored on the hard drives of personal computers, to remote servers in a domain controlled by online service providers ».[219]

En vertu de la FIPPA, l'information personnelle doit uniquement être conservée au Canada, incluant les journaux et les bandes de sauvegarde, sauf si la personne concernée a identifié ses renseignements et a donné son consentement pour qu'ils soient stockés à l'étranger ou si cela est permis en vertu de la loi :

> « 30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies: (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction; (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act; (c) if it was disclosed under section 33.1 (1) (i.1) ».[220]

---

[215] OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FOR BRISTISH COLUMBIA (ci-après : « OIPCBC »), « Cloud Computing Guidelines for Public Bodies », (2012), en ligne : < https://www.oipc.bc.ca/guidance-documents/1427 >, p. 1.

[216] *Id*.

[217] Notons que les deux acronymes « FIPPA » et « FOIPPA » sont utilisés pour l'appellation de cette loi par les organismes gouvernementaux de la Colombie-Britannique.

[218] OIPCBC, préc., note 215.

[219] *Id*., p. 1, citant Matthew NIED, « Cloud Computing, the Internet, and the *Charter* Right to Privacy : The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy », (2011) 69(5) *The Advocate* 701.

[220] *FIPPA*, art. 30.1. Voir OIPCBC, préc., note 215, p. 3-4 : « The regulations to FIPPA set out the requirements for consent under s. 30.1(a). According to the regulations, an individual's consent must be in writing and must specify the personal information for which the individual is providing consent, the date on which the consent is effective and, if applicable, what date the individual's consent expires. The consent must also specify who may store or access

Sauf exceptions prévues à la loi, les règles de la FIPPA s'appliquent à l'information personnelle qui est *sous la garde ou le contrôle* d'une institution gouvernementale[221].

Ainsi, tout employé, bénévole ou prestataire de services d'une institution gouvernementale de la Colombie-Britannique ayant sous sa garde ou son contrôle de l'information personnelle devra se conformer aux règles de la FIPPA, peu importe où les renseignements se trouvent[222]. Bien que la FIPPA ne fournit pas de définition officielle de ce que signifie *sous la garde et le contrôle* d'une institution gouvernementale, le CIVPCB est d'avis que :

> « Determining who has custody or control of personal information can be challenging and depends on a variety of circumstances. FIPPA only applies to personal information that is "in the custody or under the control of" a public body. For example, if while working, a librarian posts photos of his vacation on his social networking profile, it is unlikely those photos would be considered to be "in the custody or under the control of" the library. By contrast, if the librarian posts photos of people reading magazines in the library on the library's social networking page, it is likely those photos would be considered to be in the custody or under the control of the library ».[223]

Bref, peu importe la définition retenue, dès qu'un renseignement personnel est sous la garde ou le contrôle d'institution gouvernementale, la FIPPA interdit qu'il soit conservé ou qu'on y permette l'accès à l'extérieur du Canada. Ceci représente évidemment un enjeu économique important puisque plusieurs compagnies offrent le traitement et le stockage de l'information à l'extérieur du Canada[224].

---

the personal information from outside of Canada, and if it is practicable, which jurisdiction the personal information may be stored in or accessed from. The consent must also specify the purpose of storing or accessing the personal information » [Nos soulignements].

[221] *FIPPA*, art. 1 : « This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following [...] ».

[222] OIPCBC, préc., note 215, p. 3.

[223] *Id.*, p. 2.

[224] *Id.*, p. 3.

i) Contraintes juridiques

En 2004, le CIVPCB a étudié les implications du *USA PATRIOT Act* sur l'externalisation de l'information personnelle à l'étranger dans son Rapport intitulé « Privacy and the USA Patriot Act Implications for British Columbia Public Sector Outsourcing »[225]. Le Commissaire a été saisi du dossier suite à l'adoption du *USA PATRIOT Act* afin de faire la lumière sur les conséquences de cette loi pour la vie privée des citoyens de la Colombie-Britannique. De plus, une poursuite intentée devant la Cour suprême de la Colombie-Britannique contre le ministère de la Santé[226] avait suscité des inquiétudes à cet égard : le ministère sous-traitait la gestion de son programme d'assurance santé publique avec un prestataire de services établi aux États-Unis. Ainsi, les renseignements personnels de santé des citoyens étaient accessibles aux autorités américaines en vertu de l'article 215 du *USA PATRIOT Act*.

Le Commissaire devait répondre aux deux questions suivantes :

1. Est-ce que la *USA PATRIOT Act* permet aux autorités américaines d'accéder à l'information des citoyens de la Colombie-Britannique via l'externalisation de services publics sous la garde ou le contrôle d'un prestataire de services privé basé aux États-Unis ? Dans la positive, quelles sont les conditions d'accès ?

2. Quelles sont les implications pour une institution gouvernementale qui se conforme aux règles de protection des renseignements personnels prévues à la FOIPPA et quelles mesures peuvent être suggérées pour éliminer ou mitiger les risques pour la vie privée affectant la FOIPPA ?

En 2001, l'article 215 du *USA PATRIOT Act* a amendé la *Foreign Intelligence Surveillance Act of 1978* (« FISA »)[227] pour permettre aux autorités américaines d'obtenir des renseignements ou tout autre « chose tangible » dans le but de se protéger contre les activités terroristes internationales et clandestines. De plus, l'article 505 du *USA PATRIOT Act* a étendu les circonstances en vertu desquelles le FBI peut remettre des « lettres de sécurité nationale » aux États-Unis pour forcer les institutions financières, les entreprises de télécommunication et les

[225] OIPCBC, « Privacy and the USA Patriot Act, Implications for British Columbia Public Sector Outsourcing », (2004), en ligne : < http://www.oipc.bc.ca/special-reports/1271 >.

[226] *B.C.G.E.U.* v. *British Columbia (Minister of Health Services),* 2007 BCCA 379.

[227] *Foreign Intelligence Surveillance Act of 1978*, 50 U.S. Code Chapter 36.

prestataires de service Internet à divulguer des renseignements concernant leurs consommateurs ou clients[228]. Ainsi, le FBI doit seulement établir que l'information visée est pertinente à une enquête autorisée pour obtenir l'accès à de tels renseignements[229].

En décembre 2001, la *Loi anti-terroriste*[230] canadienne a été adoptée et a amendé plusieurs autres lois canadiennes. Certaines infractions terroristes ont été ajoutées au *Code criminel*[231] et la définition de « menace pour la sécurité au Canada » a été amendée dans la *Loi sur le Service canadien du renseignement de sécurité*[232] (« Loi sur le SCRS »). Même avant cet amendement, la Loi sur le SCRS accordait à celui-ci un généreux mandat de collecte de renseignements sur les citoyens, que ce soit au Canada ou à l'étranger, et des pouvoirs de faire forcer la divulgation de ceux-ci si nécessaire[233].

En 2004, la Parlement canadien a adopté une nouvelle loi sur la sécurité publique[234] dont certaines parties ne sont cependant pas encore en vigueur. La Loi a pour objet d'étendre les pouvoirs d'enquête de la police et de changer certaines autres lois afin d'impliquer le secteur privé dans la collecte et la divulgation de renseignements personnels à des fins nationales ou autres. De la même manière, les amendements à la *LPRPDÉ* permettent aux organisations privées

---

[228] Notons que, comme nous le verrons plus loin, la loi interdit aux entreprises contraintes de divulguer des renseignements en vertu desdites « lettres de sécurité nationale » d'aviser les personnes visées par cette demande de divulgation. En effet, l'article 1861(d) de la FISA prévoit que : « no person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section ». Voir Cynthia CHASSIGNEUX, « Quand la sécurité nationale interpelle la protection des renseignements personnels : l'exemple de la USA Patriot Act », dans Service de la formation continue du Barreau du Québec, *Vie privée et protection des renseignements personnels (2006)*, Cowansville, Yvon Blais, 2006, p. 61, à la page 70.

[229] OIPCBC, préc., note 225, p. 15 et 16.

[230] *Loi antiterroriste*, LC 2001, c 41

[231] Voir Jennifer WISPINSKI, « La « PatriotAct » des États-Unis et la *Loi Antiterroriste* du Canada : Principales différences entre les deux approches législatives », (2006), en ligne : < http://www.parl.gc.ca/content/lop/researchpublications/ prb0583-f.pdf >.

[232] *Loi sur le service canadien du renseignement de sécurité,* L.R.C. 1985, c. C-23.

[233] OIPCBC, préc., note 225, p. 16.

[234] *Public Safety Act*, 2002, SC 2004, c 15 ; OIPCBC, préc., note 225, p. 16.

de collecter et de divulguer les renseignements personnels de clients ou consommateurs à des fins de sécurité nationale ou pour exécuter la loi[235].

Sur la première question, le commissaire a conclu que, si l'information se trouve à l'extérieur du Canada, elle sera sujette aux lois s'appliquant là où elle se trouve[236]. Cette règle s'appliquera donc à tout contrat d'impartition, d'externalisation ou de services infonuagiques où les renseignements sont conservés aux États-Unis ou par une compagnie établie aux États-Unis. Sur ce dernier point, il a déjà été conclu par les tribunaux américains qu'une compagnie américaine aura le contrôle d'une compagnie étrangère si elle peut, directement ou indirectement, élire une majorité d'administrateurs[237]. Dans ce contexte, l'information détenue par une telle compagnie sera sujette au *USA PATRIOT Act*. Le CIVPCB ajoute :

> « We are inclined to the view, for the reasons described in Chapter 10, that there is a reasonable possibility of the FIS Court issuing a FISA order affecting personal information of British Columbians located in British Columbia – a possibility that has increased as a result of the *USA Patriot Act* amendments to FISA. Section 215 of the *USA Patriot Act* removed the limits to the types of organizations that can be investigated under FISA orders. Further, ongoing concerns about terrorism increase the likelihood that, when the FIS Court applies a 'balancing test' in reviewing applications for FISA orders, it may give greater weight to US national security concerns than to Canadian concerns about privacy protection ».[238]

Quant à la deuxième question, le CIVPCB a répondu que les institutions gouvernementales de la Colombie-Britannique doivent, directement ou via leurs sous-traitants, mettre en place des mesures de sécurité raisonnables pour protéger les renseignements personnels de ses citoyens à l'encontre d'un ordre extraterritorial de la FISA ou d'une lettre de sécurité nationale américaine :

> « As for the second question posed in the Request for Submissions, we concluded in Chapter 9 that disclosure by a public body or a contractor for the purpose of complying with a FISA order (or a national security letter) is unauthorized disclosure under sections 30 and 33 of FOIPPA. FOIPPA, as we

[235] OIPCBC, préc., note 225, p. 16.

[236] *Id.*, p. 132.

[237] *Id.*

[238] *Id*. p. 133.

> discussed, requires public bodies, directly and through their contractors, to implement reasonable, but not absolute, security arrangements to protect personal information against risks, including risk of unauthorized disclosure in response to an order made under foreign law ».[239]

Suite à ces réponses, le CIVPCB a émis une série de recommandations (16) au gouvernement de la Colombie-Britannique. Sans toutes les résumer, nous en dégagerons les principes que nous jugeons les plus importants aux fins de la présente étude.

ii) Recommandations

En premier lieu, le CIVPCB propose une série d'amendements à la FOIPPA, telle qu'une obligation explicite pour un contractant de notifier à une institution gouvernementale toute divulgation non autorisée de renseignements personnels. Le Commissaire recommande également qu'une responsabilité directe soit attribuée au contractant afin que l'information personnelle soit uniquement collectée et divulguée de manière conforme à la FOIPPA[240].

Ensuite, il indique que le gouvernement de la Colombie-Britannique devrait rédiger une « published litigation policy » en vertu de laquelle il pourrait participer ou entamer des procédures judiciaires au Canada ou à l'étranger afin de s'opposer à tout *subpoena*, mandat, ordre, requête ou autre demande de divulgation faite par une autorité étrangère envers une institution de la Colombie-Britannique qui a la garde ou le contrôle de renseignements personnels[241]. Il ajoute, aux recommandations 7 et 8, que le gouvernement du Canada devrait revoir la législation tant fédérale que provinciale de manière à ce qu'elle protège adéquatement les renseignements personnels qui sont sous la garde ou le contrôle du gouvernement canadien ou d'une province contre une demande de divulgation étrangère. Selon le CIVPCB, le gouvernement de la Colombie-Britannique devrait d'ailleurs, en collaboration avec le gouvernement canadien,

---

[239] *Id.*

[240] *Id.*, p. 135.

[241] *Id.*

solliciter auprès des autorités américaines appropriées une assurance qu'elles ne vont pas chercher à accéder aux renseignements personnels détenus en Colombie-Britannique[242].

Le CIVPCB a également indiqué que toutes les institutions gouvernementales de la Colombie-Britannique devraient s'assurer qu'elles engagent, pour la durée des contrats en cause, les ressources financières et autres ressources nécessaires pour activement et diligemment surveiller la réalisation de leurs obligations contractuelles, détecter et punir toute violation, et pour se défendre contre toute divulgation actuelle ou potentielle de l'information personnelle devant une cour d'un pays étranger ou toute autre autorité étrangère[243].

Le CIVPCB précise qu'il n'est pas suffisant de se fier aux contractants pour rapporter les problèmes ou les divulgations non autorisées. Une institution qui a externalisé ses données devrait créer et implanter un programme régulier d'audit de conformité. De tels audits devraient être réalisés par un tiers auditeur possédant l'expertise requise et être sélectionnés par l'institution[244]. Les recommandations 9 à 12 expliquent précisément à quels niveaux les audits de conformité devraient être effectués par les institutions gouvernementales.

Par ailleurs, le CIVPCB est d'avis que le Conseil du trésor devrait diriger tout ministère, agence et organisations sujettes au *Budget Transparency and Accountability Act*[245] de manière à inclure, dans leurs planifications annuelles, les activités proposées aux recommandations 4 et 5 et de prévoir les ressources nécessaires pour les réaliser. Il est également d'avis que le gouvernement de la Colombie-Britannique devrait exiger de ses institutions qu'elles soumettent un plan et un budget à cet égard[246].

Parmi les autres recommandations, il est suggéré au gouvernement canadien que des ententes internationales, publiques et économiques soient conclues afin de protéger les renseignements

---

[242] *Id.,* p. 136.

[243] *Id.*

[244] *Id*.

[245] SBC 2000, c 23.

[246] OIPCBC, préc., note 225, p. 136.

personnels et les droits fondamentaux[247]. Il est finalement recommandé que le gouvernement canadien et le gouvernement de la Colombie-Britannique se penchent également sur toutes ces questions pour le secteur privé[248].

c) La Saskatchewan

Le Commissaire à l'information et à la vie privée de la Saskatchewan (ci-après, le : « CIVPS ») a récemment rendu ses conclusions quant à un sondage effectué par le gouvernement de la Saskatchewan auprès de ses employés et pour lequel les données recueillies étaient hébergées aux États-Unis[249].

En vertu de l'article 33 de la *Freedom of Information and Protection of Privacy Act* (ci-après la « FOIP »), le CIVPS a été saisi pour enquêter sur la conservation aux États-Unis de renseignements personnels collectés lors d'un sondage effectué par la Public Service Commission (ci-après « PSC ») et sur la juridiction du *USA PATRIOT Act*. Dans le cadre de ce sondage, la PSC recueillait des renseignements sur les responsabilités professionnelles des employés, leurs tâches accomplies dans un ancien emploi, leur nom, leur adresse de résidence, leur numéro d'employé et leur numéro de téléphone personnel. Selon le Rapport, l'information collectée par la PSC lors du sondage l'était à des fins de « redéploiement en cas de circonstances significatives »[250]. Le Commissaire a aussi été informé que la PSC de la Saskatchewan faisait héberger aux États-Unis l'information contenant les applications de candidats à des offres d'emploi[251].

i) Contraintes juridiques

L'enquête a révélé que l'information collectée par la PSC était hébergée par une compagnie (« Compagnie X ») établie aux États-Unis et offrant des services en technologies de

[247] *Id.*, p. 140.

[248] *Id.*, p. 139.

[249] *Public Service Commission (Re)*, 2013 CanLII 55439 (SK IPC).

[250] *Id.*, par. 2.

[251] Voir : GOVERNMENT OF SASKATCHEWAN, « The Career Centre », en ligne : < www.careers.gov.sk.ca/ >.

l'information. Il appert que l'information hébergée par la Compagnie X était donc sujette aux lois américaines, incluant le *USA PATRIOT Act*[252].

La PSC a indiqué au Commissaire qu'elle avait choisi cette compagnie pour héberger les données, car elle offrait le meilleur véhicule de collecte des données, tel qu'une bonne disponibilité, des coûts moindres et un service convivial et facilement mis à jour. De plus, les modalités de recherche et d'accès aux données rendaient le service facile d'utilisation[253].

Le contrat conclu entre le PSC et la Compagnie X avait été signé en 2002 et a été renouvelé en 2006. En 2010, il a été renouvelé de nouveau et a été amendé, de manière à ce que la PSC reçoive notification quand 1) la Compagnie X reçoit une demande de divulguer l'information personnelle à une tierce partie, et 2) quand un bris de confidentialité de l'information confidentielle est survenu. De plus, l'amendement stipule que les employés de la compagnie vont seulement avoir accès aux données de façon pertinente à l'exécution du contrat (« on a "need-to-know" basis ») et que l'information confidentielle sera retournée à la PSC ou détruite lors de l'expiration du contrat[254].

En vertu du contrat conclu entre les parties, il appert ainsi que la Compagnie X avait le droit de sous-traiter les services sans en notifier la PSC[255] :

> « The above provisions do not require Company X to notify PSC if Company X subcontracts any of the services it delivers to PSC. Effectively, excluding PSC from the subcontracting process hinders and disables PSC's ability to maintain control over the information. For example, as far as PSC is aware, the information is transferred and stored in the USA. However, if Company X subcontracts with another company to store the information, the information can be transferred to yet another jurisdiction and therefore, subject to further foreign legislation ».[256]

---

[252] *Public Service Commission (Re)*, préc., note 249, par. 5.

[253] *Id.,* par. 9.

[254] *Id.,* par. 45.

[255] *Id.,* par. 117.

[256] *Id.*

Il importe de souligner que le site des offres d'emploi indiquait aux candidats que leurs renseignements personnels étaient conservés aux États-Unis : « Please be aware that the information in your application will be stored electronically on a server in the U.S.A. The information will be protected with appropriate security safeguards, but may be subject to U.S. laws »[257].

Le CIVPS indique toutefois que la notification de la PSC à l'effet que l'information des candidats est protégée par des mesures de sécurité appropriées est inexacte[258]. Au contraire, il est d'avis que, à l'extérieur du Canada, les renseignements personnels des employés et candidats ne sont pas adéquatement protégés[259]. Ainsi, le CIVPS a conclu que la PSC ne disposait pas de mesures de sécurité adéquates pour la protection des renseignements personnels collectés lors du sondage et se trouvant sur son site d'offres d'emploi. De plus, même si la FOIP n'interdit pas le transfert de renseignements personnels à un prestataire de services établi aux États-Unis, les institutions gouvernementales de la Saskatchewan ont le devoir de protéger les renseignements personnels dont elles ont la garde et le contrôle[260]. Le Commissaire indique que la Colombie-Britannique est également de cet avis et cite le rapport « Privacy and the *USA Patriot Act* : Implications for British Columbia Public Sector Outsourcing »[261], à l'égard de la *Freedom of Information and Protection of Privacy Act* (« FOIPPA ») :

> « The fact that outsourcing is contemplated by FOIPPA does not, however, authorize a public body to do so in circumstances that would reduce security arrangements for personal information below those required of the public body directly. A public body cannot contract out of FOIPPA either directly or by outsourcing its functions. The decision to outsource does not change the public body's responsibilities under FOIPPA. Nor does it change public and individual rights in FOIPPA, which are not balanced against any 'right' to outsource ».[262]

---

[257] *Id*.

[258] *Id.,* par. 119.

[259] *Id*.

[260] *Id.,* par. 10.

[261] OIPCBC, préc., note 225, p. 100.

[262] *Public Service Commission (Re)*, *préc.*, note 249, par. 11, citant : OIPCBC, *préc.*, note 225, p. 100.

De la même manière, il indique que l'Ontario a aussi évoqué des conclusions en ce sens :

> « The critical question for institutions which have outsourced their operations across provincial or international borders is whether they have taken reasonable steps to protect the privacy and security of the records in their custody and control. I have always taken the position that you can outsource services, but you cannot outsource accountability ».[263]

Ainsi, les institutions gouvernementales de la Saskatchewan doivent prendre les moyens appropriés pour gérer et protéger les renseignements personnels lorsqu'ils externalisent le traitement de renseignements par le biais d'une compagnie étrangère, afin de se conformer à la FOIP et à la *Local Authority Freedom of Information and Protection of Privacy Act*[264].

ii) Recommandations

Sur la base de ces faits, le Commissaire à l'information et à la vie privée de la Saskatchewan a émis plusieurs recommandations à l'intention du PSC et à l'égard du contrat conclu avec la Compagnie X.

D'une part, le Commissaire recommande que le contrat conclu entre les parties soit amendé afin de déterminer 1) le responsable de la destruction de l'information; 2) la manière dont celle-ci sera détruite; et 3) des calendriers spécifiques de destruction des documents[265]. Il recommande en outre que le contrat soit modifié de manière à stipuler qu'aucun document ne pourra être détruit s'il fait l'objet d'une demande d'accès à l'information ou de rectification et ce, à l'intérieur d'un délai d'appel d'un an[266]. La PSC devrait aussi envoyer une notification claire aux employés et aux candidats à un emploi à l'effet que leurs renseignements personnels ne pourront être adéquatement protégés à l'étranger[267].

---

[263] *Public Service Commission (Re)*, *préc.*, note 249, par. 12, citant : ONTARIO INFORMATION AND PRIVACY COMMISSIONER, « Privacy Investigation Report PC12-39: Reviewing the Licensing Automation System of the Ministry of Natural Resources: A Special Investigation Report », (2012) p. 6.

[264] *Public Service Commission (Re)*, *préc.*, note 249, par. 13.

[265] *Id.*, par. 146 et 147.

[266] *Id.*, par. 148.

[267] *Id.*, par. 152.

Le PSC devrait, d'autre part, déterminer et documenter ses propres normes et pratiques de sécurité, de manière conforme à la FOIP, au *Health Information Protection Act*[268], et au *Overarching Personal Information Privacy Framework for Executive Government*[269]. Par la suite, le PSC devra évaluer si les politiques de sécurité et les pratiques de la Compagnie contractante respectent les conditions prévues au FOIP[270].

Par ailleurs, le CIVPS est d'avis que les contrats conclus entre les institutions gouvernementales et les contractants devraient généralement stipuler que 1) la sous-traitance ou le transfert de l'information doit être préalablement approuvé par l'institution gouvernementale[271], et 2) les contractants sont obligés de se conformer au FOIP lorsqu'ils remplissent leurs responsabilités en vertu du contrat conclu avec l'institution gouvernementale[272].

En définitive, le CIVPS recommande au gouvernement qu'une réforme du *Freedom of Information and Protection of Privacy Act* et du *Local Authority Freedom of Information and Protection of Privacy Act* soit adoptée afin d'y inclure un devoir explicite de « protection des renseignements personnels sous la garde ou le contrôle des institutions gouvernementales »[273] et que des amendes significatives et/ou un emprisonnement soient prévus pour le non-respect de ce devoir de protection[274]. De surcroît, l'information personnelle, telle que définie à l'article 24 du FOIP, devrait être traitée conformément à la partie IV du FOIP et les institutions gouvernementales devraient la reconnaitre comme étant distincte des autres types de renseignement[275].

---

[268] SS 1999, c H-0.021.

[269] GOVERNMENT OF SASKATCHEWAN, « An Overarching Personal Information Privacy Framework for executive Government », (2003), en ligne : < http://www.publications.gov.sk.ca/redirect.cfm?p=32639&i=39659 >.

[270] *Public Service Commission (Re)*, préc., note 249, par. 145.

[271] *Id*., par. 149.

[272] *Id*., par. 4.

[273] *Id*., par 152.

[274] *Id*., par 4.

[275] *Id*.

2) Les exemples internationaux

Notre analyse de l'utilisation de l'infonuagique par des gouvernements étrangers a évidemment été limitée par des barrières linguistiques. Ainsi, seuls les pays ayant publié leurs politiques en français ou en anglais ont retenu notre attention. Parmi ceux-ci, nous avons opté pour trois pays de common law ayant des régimes similaires au Canada, soit l'Australie (a), le Royaume-Uni (b) et les États-Unis (c), notamment parce que la documentation disponible sur les tentatives d'adoption de stratégies infonuagiques dans ces états était particulièrement facile d'accès[276]. Bien que nous admettons qu'il aurait été utile d'étudier les politiques d'infonuagique de pays de droit civil tels la France ou la Belgique, l'absence d'une documentation suffisante accessible dans les délais impartis à la préparation de la présente étude nous a forcé à écarter ces pays de notre bassin d'analyse.

a) L'Australie

Le gouvernement australien a su identifier plusieurs avantages associés à la mise en place d'une stratégie d'infonuagique gouvernementale. Il a notamment été considéré que l'infrastructure du nuage pourrait apporter des avantages substantiels pour le gouvernement en termes de simplicité, de coût, de sécurité, de flexibilité et de rythme d'innovation[277]. Pour le gouvernement australien, l'un des principaux avantages d'un modèle de services infonuagiques découle du fait qu'il permet d'offrir une flexibilité permettant de faire évoluer facilement le niveau de service requis en fonction des besoins de l'organisation visée[278]. Pour le reste, les arguments invoqués reprennent en quelque sorte ceux mis de l'avant dans la première partie de la présente étude :

- L'infonuagique peut permettre au gouvernement d'offrir des services informatiques d'une manière plus efficace et plus rentable.

---

[276] Il est d'ailleurs à noter que ces trois mêmes pays ont fait l'objet d'une analyse sommaire par le Laboratoire d'étude sur les politiques publiques et la mondialisation (LEPPM). Voir M. TREMBLAY, préc., note 15.

[277] GLOBAL ACCESS PARTNERS, « GAP Task Force on Cloud Computing », (2011) : en ligne : < http://www.globalaccesspartners.org/Cloud-Computing-GAP-Task-Force-Report-May-2011.pdf >, p. 13.

[278] AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE, « Negotiating the Cloud – Legal Issues in Cloud Computing Agreements » (2013), en ligne : < http://agict.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf >, p. 14.

- L'adoption de services infonuagiques par le gouvernement rendra possible la diffusion des applications par Internet, via un navigateur Web.
- Les applications et les données seront stockées de manière centralisée et conçues pour être utilisées à partir d'infrastructures partagées, hautement évolutives, sécurisées et fiables.
- Des appareils tels que les ordinateurs portables, les tablettes et les téléphones intelligents sont des portails vers les données qui aideront les gens à être productifs depuis n'importe quel emplacement et à n'importe quel moment.
- Les mises à jour ne sont pas nécessaires pour accéder à l'innovation la plus récente – une simple actualisation du navigateur suffira.
- Les entreprises et les gouvernements n'auront plus besoin de posséder ou de gérer des serveurs et des logiciels clients; ils achèteront plutôt des applications intégrées et des plateformes de développement d'autres entités, et pourront ainsi consacrer leur temps à l'amélioration des processus internes et à la prestation de service[279].
- Le recours à l'infonuagique pourrait réduire les coûts initiaux de dépenses en capital du matériel informatique et les dépenses connexes comme un centre de données physique et le personnel de soutien, tout en réduisant le risque financier assumé par l'agence, en remplaçant les coûts initiaux par les dépenses de fonctionnement raisonnablement prévisibles et en ne payant que pour la quantité de traitement informatique et le stockage de données utilisé par l'agence[280].
- Le recours à l'infonuagique pourrait également réduire les coûts permanents en utilisant une infrastructure et un personnel de spécialistes techniques, dont les services sont généralement partagés entre de nombreux clients, leur permettant de réaliser des économies d'échelle.

[279] GLOBAL ACCESS PARTNERS, préc., note 277, p. 13.

[280] AUSTRALIAN GOVERNMENT DEPARTMENT OF DEFENCE INTELLIGENCE AND SECURITY, « Cloud Computing Security Considerations », (2012), en ligne : < http://www.dsd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf >, p. 4.

Évidemment, le gouvernement australien a reconnu que les coûts associés à la mise en œuvre des contrôles de sécurité, notamment ceux liés à l'infrastructure partagée, auront pour effet, comme nous l'avons déjà souligné, de limiter les économies générées[281].

D'autres arguments n'ayant pas été abordés jusqu'à présent ont également été soulevés en faveur d'une stratégie infonuagique australienne, à savoir :

- Le nuage pourrait réduire les effets néfastes de la technologie sur l'environnement dus à une utilisation plus efficace du matériel informatique nécessitant moins d'électricité et moins de climatisation[282].
- L'infonuagique, associée avec une connectivité à haute vitesse, offre une possibilité d'améliorer considérablement la vitesse, la qualité et la disponibilité des services à tous les niveaux du gouvernement, mais particulièrement pour les gouvernements locaux basés dans les régions éloignées.
- L'infonuagique a un potentiel important pour améliorer l'efficacité dans l'administration locale puisqu'il permet l'utilisation de solutions sophistiquées par des organismes gouvernementaux régionaux qui n'ont pas le budget requis pour les instaurer eux-mêmes.
- L'infonuagique peut offrir aux agences gouvernementales la possibilité de traiter des demandes inattendues avec plus d'efficacité dans des situations d'urgence civile. En effet, les systèmes existants n'ont pas été construits pour pouvoir gérer une demande si considérable et rare et l'infonuagique offre une solution évidente à ce problème[283].

Sinon, il importe de préciser que l'Australie recourt déjà à l'utilisation de l'infonuagique pour un certain nombre de données qui sont déjà dans le domaine public (services citoyens, information du public, etc.). L'hébergement de ces données dans le nuage aura permis l'ouverture des données publiques gouvernementales, tel que le recommandait le rapport du *Gov 2.0 Task Force*. En effet, comme les données publiques n'ont pas à être hébergées sur les serveurs du gouvernement (leur

[281] *Id.*

[282] *Id.*

[283] GLOBAL ACCESS PARTNERS, préc., note 277, p. 13.

confidentialité n'étant pas requise), de nombreux sites Web des ministères pourraient techniquement être hébergés dans le nuage. C'est d'ailleurs ce qui a été mis de l'avant dans le rapport *Cloud Computing Strategic Direction* du gouvernement australien, lequel favorise la transition des sites publics vers l'environnement infonuagique. Ainsi, des sites tels que < www.data.gov.au > sont déjà hébergés dans le nuage[284].

i) Contraintes juridiques

Selon les politiques en place, lorsqu'une agence gouvernementale australienne considère un transfert de ses données vers un environnement infonuagique, elle doit répondre à une série de questions au-delà de celles du coût des services et de la flexibilité. Celles-ci incluent les risques liés à la protection de la vie privée, à la performance et la sécurité, ainsi que le temps de latence inhérent causé par le transfert du trafic Internet australien via des serveurs situés à travers le monde. L'interopérabilité, la fiabilité, les normes, les contrats, la performance, les stratégies de sortie et les contraintes législatives et réglementaires doivent également être pris en compte [285].

Les exigences de sécurité du gouvernement australien pour l'infonuagique indiquées dans le rapport du *Department of Defence* intitulé *Cyber Security Operations Centre on Cloud Computing Security Considerations* déconseillent l'approvisionnement de services et des fonctions des technologies de l'information et de communication à l'extérieur de l'Australie puisque, dans de tels cas, les informations peuvent être traitées ou stockées sur des territoires où les lois de protection de la vie privée et de l'information sont très différentes de celles adoptées en Australie[286]. Il peut également être possible, pour les gouvernements étrangers, d'accéder aux données d'un organisme qui sont stockées dans une juridiction étrangère ou d'accéder à l'information détenue en Australie par une société ayant une présence dans un pays étranger[287]. Par exemple, si des données sont hébergées sur un serveur aux États-Unis, le gouvernement

[284] *Id.*

[285] *Id.*, p. 14.

[286] AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE, préc., note 278, p. 18.

[287] *Id.*

américain pourrait, comme nous le verrons plus loin, y accéder selon les termes du *USA PATRIOT Act*[288].

Cette position se veut d'ailleurs conforme avec le 8e principe de la *Privacy Act 1988*[289], lequel prévoit notamment que :

> « Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***) […] the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information. »

Le déplacement des données dans le nuage signifie que celles-ci circulent en dehors du contrôle direct de l'agence et peuvent, dans certains cas, être traitées et stockées à l'extérieur de l'Australie. Différents niveaux de contrôle indirects de ces données sont possibles en fonction du type de service infonuagique choisi et des protections juridiques mises en place par l'agence gouvernementale[290]. En outre, les obligations de confidentialité des institutions gouvernementales peuvent différer de celles imposées aux prestataires de services infonuagiques et il est difficile d'externaliser des informations à une entité qui ne respecte pas les politiques qui ont été imposées à une agence gouvernementale[291]. Il importe donc d'examiner les mesures de sécurité offertes par les prestataires de services infonuagiques et de s'assurer qu'ils sont en mesure de respecter leurs obligations en matière de confidentialité (notamment en veillant à ce que toutes les copies de sauvegarde soient supprimées[292]). En effet, il revient aux agences de s'assurer que les exigences en matière de protection de l'information sont atteintes[293]. La vérification des politiques des prestataires de services infonuagiques peut servir à cette fin, mais cette vérification peut toutefois être compliquée par (1) l'emplacement des données (qui peut être inconnu à moins qu'il en soit

[288] GLOBAL ACCESS PARTNERS, préc., note 277, p. 14.

[289] No 119, 1988 as amended.

[290] AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE, préc., note 278, p. 8.

[291] *Id.*

[292] GLOBAL ACCESS PARTNERS, préc., note 277, p. 27.

[293] AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE, préc., note 278, p. 11.

autrement convenu) et (2) la nature de l'infonuagique qui peut répartir les données de l'agence à travers plusieurs supports informatiques appartenant à des prestataires distincts[294].

Finalement, le gouvernement australien a reconnu que les éléments potentiellement anticoncurrentiels de la gestion des droits numériques, ainsi que les questions d'interopérabilité des logiciels, constituaient des entraves au recours à certains services infonuagiques[295].

ii) Solution retenue

Plusieurs recommandations ont été faites par Sir Peter Gershon dans son *Review of the Australian Government's Use of Information and Communication Technology* concernant l'utilisation gouvernementale de l'infonuagique, recommandations qui ont toutes été retenues par le gouvernement. Ces recommandations comprenaient l'élaboration d'un plan stratégique pour les centres de données de l'ensemble du gouvernement, le resserrement de la gestion des dépenses en technologies de l'information et de la communication, les options à explorer pour les services partagés et l'élaboration d'un plan de développement durable des technologies de l'information et de la communication pour l'ensemble du gouvernement. Selon le rapport, un certain nombre d'organismes ont indiqué qu'ils utilisaient déjà les technologies de virtualisation, tandis que d'autres ont invoqué l'intention de les adopter. Par extension, l'adoption des services infonuagiques peut offrir des opportunités à l'examen de l'ensemble des besoins des centres de données du gouvernement, à l'amélioration de la normalisation entre les organismes, à la réduction des coûts par rapport aux technologies de l'information et de la communication, à l'optimisation des ressources et à l'amélioration de la durabilité[296].

Une autre solution proposée par le gouvernement australien est de s'attaquer aux préoccupations d'ordre juridique par l'adoption de normes communes et ouvertes par les divers prestataires de services infonuagiques afin d'améliorer la transparence, la confiance, la portabilité des données et

---

[294] *Id.*

[295] GLOBAL ACCESS PARTNERS, préc., note 277, p. 15.

[296] *Id.*, p. 14.

l'interopérabilité[297]. Le gouvernement a décidé de ne pas adopter de réglementation stricte puisqu'il estime que cela pourrait minimiser les effets bénéfiques qu'Internet et l'infonuagique puissent avoir sur l'expansion économique. D'autre part, il a été considéré que la réglementation « intelligente » peut faciliter, améliorer et accélérer les opportunités commerciales, en particulier si elle est bien informée et moins stricte dans sa nature. Il y avait donc un fort soutien à l'élaboration de codes de conduite du secteur pour couvrir les différents aspects de l'infonuagique. Les codes de conduite allégés, plutôt que la législation prescriptive, sont – selon le gouvernement australien – la voie à suivre, mais il doit y avoir un mécanisme de plainte et des mesures correctives en cas de violation d'un accord contractuel. Une approche qui est basée sur les risques et les principes a été jugée bénéfique, notamment parce qu'une telle approche a donné de bons résultats pour le secteur financier australien et a aidé l'Australie à surmonter la crise financière mondiale. Ce modèle a l'avantage d'être clair, relativement simple et efficace[298].

Le succès du code de pratique sur la cybersécurité des prestataires Internet australiens est un bon exemple d'autorégulation efficace initiée par le gouvernement. Il consiste à éduquer les consommateurs et à encourager les prestataires Internet, dans leur propre intérêt, à adopter une approche commune et offre ainsi un modèle pour la réglementation des nuages. Toutefois, ces codes doivent faire partie d'un cadre cohérent basé sur des principes pour éviter la fragmentation ou une pléthore de régimes déroutants[299].

Plusieurs autres initiatives ont été entreprises par le gouvernement australien. Il a notamment développé une stratégie de centre de données basée en partie sur le modèle IaaS. Selon les projections fournies, la rationalisation des centres de données entraînera des économies substantielles dans les coûts et la consommation d'énergie et, en même temps, permettra d'améliorer les normes de service et d'augmenter la capacité de faire face aux perturbations[300]. Le

[297] *Id.*, p. 25.

[298] *Id.*, p. 32.

[299] *Id.*

[300] GOVERNMENT OF AUSTRALIA, DEPARTMENT OF FINANCE AND DEREGULATION, « Cloud Computing Strategic Direction Paper: Opportunities and Applicability for Use by the Australian Government », (2013), en ligne :< http://agimo.gov.au/files/2012/04/final_cloud_computing_strategy_version_1.pdf >, p. 28.

gouvernement australien a par ailleurs adopté, en novembre 2009, une *Cyber Security Strategy*, laquelle énonce les objectifs de sa politique de cybersécurité, ainsi que les priorités stratégiques à poursuivre pour atteindre ces objectifs. La stratégie décrit également les actions et les mesures qui seront prises à travers l'ensemble du gouvernement australien pour atteindre ses priorités stratégiques[301]. En outre, le gouvernement australien a abordé de nombreux problèmes de confidentialité dans ses treize nouveaux principes *Australian Privacy Principles* (« APP »), qui entreront en vigueur à partir de mars 2014 et qui s'appliqueront à la fois au secteur public et au secteur privé. L'APP est structuré pour refléter le cycle de vie de l'information, prenant en compte la notification, la collection, l'utilisation, la divulgation, la sécurité, l'accès et la rectification[302].

b) Le Royaume-Uni

Le gouvernement du Royaume-Uni s'est récemment doté d'un « G-cloud », soit un réseau d'infonuagique à l'échelle gouvernementale[303]. Cette initiative s'inscrivait dans la mise en place de la « Government Cloud Strategy » rendue publique en 2011[304] et faisait suite à différents rapports d'organismes publics dont le *Digital Britain Report*, publié en juin 2009 par le *Department for Business Innovation & Skills* et le *Department for Culture, Media and Sport*[305], lequel rapport invitait le gouvernement britannique à mettre en place une stratégie numérique de grande envergure pour le pays. Suite à la publication du rapport, le Premier Ministre Gordon Brown s'est dit d'avis que : « Digital Britain is about giving the country the tools to succeed and

---

[301] *Id.*

[302] *Id.*, p. 14.

[303] « Digital Britain commits government to cloud computing », (2009) *Computing,* en ligne : < http://www.computing.co.uk/ctg/news/1816113/digital-britain-commits-government-cloud-computing >.

[304] HM GOVERNMENT, « Government Cloud Strategy », (2011), en ligne : < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf >.

[305] DEPARTMENT FOR CULTURE, MEDIA and SPORT AND DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS, « Digital Britain: The Final Report », (2009), en ligne : < http://webarchive.nationalarchives.gov.uk/+/http:/www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf >.

lead the way in the economy of the future »[306]. Un aspect important de la stratégie *Digital Britain* est d'améliorer les services TI gouvernementaux et de permettre la migration en ligne de certains services. Afin de soutenir cette action, les efforts de l'approvisionnement en TI du Royaume-Uni ont été axés sur le développement du gouvernement en tant que force dirigeante de l'utilisation de l'infonuagique gouvernementale. Le rapport indique notamment que :

> [TRADUCTION] « l'incidence du gouvernement sur l'économie numérique va bien au-delà de son rôle de créateur de politiques. Dans la prestation de services publics, en tant que client important de produits et services de TIC et en tant que propriétaire des systèmes de données, le secteur public a une influence énorme sur le marché. Dans de nombreux domaines, comme l'éducation, la santé et la défense, le gouvernement peut utiliser sa position de prestataire de services initiaux pour conduire des normes – et, dans certains cas, établir des normes – et fournir un cadre d'investissement pour la recherche et le développement. »[307]

Plusieurs arguments ont été avancés par le gouvernement du Royaume-Uni afin de justifier le recours à l'infonuagique, la plupart desquels sont similaires à ceux précédemment identifiés dans la présente étude. Toutefois, il importe de préciser que, en ce qui a trait aux réductions de dépenses en TI[308], le gouvernement du Royaume-Uni aurait déjà économisé £300 millions par la migration dans le nuage, notamment grâce à la possibilité, pour les différents ministères, de partager les solutions TI[309] et, ainsi, d'éviter de gaspiller des ressources[310]. Ceci permettrait par ailleurs de répondre à l'évolution des besoins opérationnels des citoyens[311] de manière plus flexible, personnalisée et réactive[312].

---

[306] DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS, « Building Britain's Digital Future », (2009), en ligne : < http://webarchive.nationalarchives.gov.uk/20090930121249/bis.gov.uk/building-britains-digital-future# >.

[307] *Id.*

[308] HM GOVERNMENT, « Government ICT Strategy – Strategic Implementation Plan », (2011), en ligne : < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266169/govt-ict-sip.pdf >., p. 17.

[309] *Id.*

[310] *Id.*; CABINET OFFICE, « Government ICT Strategy », (2011), en ligne : < https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf >, p. 8.

[311] CABINET OFFICE, préc., note 308, p. 14.

[312] *Id.*

Comme le gouvernement australien, le gouvernement du Royaume-Uni a créé un portail unique via lequel les citoyens peuvent accéder aux services publics, aux services transactionnels (tels que les prêts étudiants ou l'allocation de demandes d'emploi) et à l'information liée au gouvernement, réduisant ainsi le temps qui doit être consacré par lesdits citoyens à la gestion de ces divers dossiers[313]. Ce portail est également utilisé par le gouvernement pour communiquer plus efficacement avec les citoyens par le biais des médias sociaux et de pétitions en ligne, permettant ainsi d'accroitre la participation citoyenne aux grands débats politiques[314]. De plus, ce portail est utilisé par le secteur public pour accroître la collaboration par le biais de conférences vidéo et téléphoniques[315].

i) Contraintes juridiques

Les contraintes juridiques identifiées par le gouvernement du Royaume-Uni sont similaires à celles identifiées par le gouvernement australien, notamment en ce qui a trait à la sécurité informationnelle[316], à la fragmentation des données dans le nuage et la possibilité que certaines données soient stockées en dehors du Royaume-Uni[317]. Le gouvernement du Royaume-Uni a par ailleurs exprimé certaines préoccupations quant aux garanties de niveau de service. En effet, puisque les services infonuagiques ne sont pas directement sous son contrôle, le gouvernement doit se fier aux prestataires pour assurer la disponibilité des services fournis aux citoyens. Or, comme nous l'avons déjà souligné, ces mêmes prestataires n'exercent aucun contrôle sur le délai de transit des données[318] et ne peuvent donc offrir aucune garantie à cet effet.

---

[313] *Id.*, pp. 18 et 19.

[314] *Id.*, p. 19.

[315] *Id.*, p. 21.

[316] *Id.*

[317] *Id.*

[318] Le délai de transit est la « [q]uantité de temps qu'on doit compter pour qu'un signal effectue le trajet d'un point à un autre dans un réseau de télécommunication ». Voir OLF, préc., note 3.

Un autre défi identifié par le gouvernement du Royaume-Uni est lié aux systèmes hérités[319], lesquels sont souvent incompatibles avec la virtualisation offerte par l'infonuagique. Comme ces systèmes jouent fréquemment un rôle critique au sein de l'infrastructure étatique, ils empêchent une migration complète vers le nuage.

Finalement, le gouvernement du Royaume-Uni a été confronté à la problématique des licences, ou, plus exactement, la transférabilité des licences d'entreprise, de sorte qu'elles puissent être exécutées dans le nuage.

ii) Solution retenue

Une nouvelle structure de gouvernance a été créée afin d'instaurer et de contrôler la stratégie infonuagique élaborée par le gouvernement du Royaume-Uni. Cette structure se compose de divers comités qui ont été créés pour répondre à différents objectifs. L'un de ces comités est responsable de la création d'un forum pour l'examen et la prise de décision, afin de s'assurer que les infrastructures de TIC du gouvernement sont utilisées de manière à contribuer le plus efficacement possible à la réforme du secteur public. Un autre comité sert à livrer et mettre en œuvre des stratégies de TIC. En outre, ces divers comités ont pour mandat de développer des solutions innovatrices, de scruter, de mesurer et de faire respecter les normes et les mesures prescrites, d'identifier des solutions performantes et de mener à leur adoption, etc. Finalement, ils devront coordonner les ententes conclues avec les prestataires de services afin de marchander les services et de livrer de meilleurs résultats commerciaux pour le gouvernement[320].

Les obligations des prestataires incluront également la gestion des risques de sécurité. Le recours à des organismes fiables pour assurer la sécurité des services infonuagiques permettra à la fois aux prestataires de services et aux consommateurs de comprendre les risques et les contre-mesures associés à l'utilisation de l'infonuagique. L'organisation qui détient les informations hébergées dans le nuage sera responsable des risques liés à la sécurité de l'information. Les

[319] Un système hérité est un « [s]ystème informatique issu d'une génération précédente de système informatique et qui continue d'être utilisé, après avoir été adapté à un système plus contemporain ». Voir OLF, préc., note 3.

[320] CABINET OFFICE, préc., note 308, p. 24.

assurances et l'accréditation du gouvernement aideront les titulaires de l'information à mitiger leurs risques[321]. En outre, pour éviter que les données ne soient accessibles sans autorisation, elles seront hébergées dans un environnement sécurisé, le système sera accrédité et l'accès y sera contrôlé[322].

En plus des obligations imposées aux divers comités faisant partie de la nouvelle structure de gouvernance, les départements ministériels seront tenus de prendre certaines mesures afin de préserver l'intégrité de leurs données. Pour ce faire, et afin de réduire les erreurs, les départements ministériels seront tenus, lorsqu'ils hébergent leurs propres données dans le nuage, de procéder eux-mêmes aux modifications requises le cas échéant. Un outil permettant de gérer le document tout au long de son cycle de vie et permettant la création de liens avec des sources de données existantes, afin d'assurer que les documents puissent être retracés, sera mis à leur disposition[323].

c) Les États-Unis

Le gouvernement fédéral américain est l'un des plus grands utilisateurs d'infonuagique communautaire sur le globe[324]. En effet, l'infonuagique a permis au gouvernement de déployer rapidement des programmes très spécifiques, tels que Forms.gov (pour tous les formulaires fédéraux), Cars.gov (pour le programme de la « prime à la casse ») et Flu.gov, lesquels sont tous liés au portail Web officiel du gouvernement américain, USA.gov. En octobre 2010, le *US General Services Administration* a sélectionné le prestataire de services infonuagiques *Enomaly* pour fournir des services IaaS aux autorités fédérales, étatiques et locales sur l'infrastructure infonuagique du gouvernement, Apps.gov[325].

Avant la migration vers le nuage, le gouvernement fédéral états-unien avait lancé une initiative concernant l'utilisation du nuage afin de créer une entreprise fédérale plus agile par laquelle les

[321] HM GOVERNMENT, préc., note 304, p. 19.

[322] HM GOVERNMENT, préc., note 308, p. 20.

[323] *Id.*

[324] Sean MARSTON *et al.*, « Cloud Computing – The Business Perspective », (2011) 51 *Decision Support Systems* 176, 180.

[325] *Id.*

services gouvernementaux pouvaient être réutilisés et fournis sur demande pour rencontrer les besoins du monde des affaires[326]. Cette initiative visait à développer une solution « e-Gouvernement » universelle basée sur une infrastructure infonuagique, sur laquelle les ressources et les outils informatiques seraient partagés uniformément entre les agences gouvernementales et les citoyens en accroissant le niveau de participation[327].

Les besoins identifiés par le gouvernement américain sont similaires à ceux identifiés par le gouvernement de l'Australie et le gouvernement du Royaume-Uni, notamment en ce qui concerne les avantages financiers procurés par l'infonuagique[328] (qui a réduit les coûts d'entretien Web par 50 %[329]), la possibilité de communiquer et collaborer plus efficacement avec les citoyens[330], ainsi que l'utilisation du nuage pour la collaboration des organismes dans le secteur public[331]. L'élasticité, l'évolutivité et l'agilité de l'infonuagique ont également influencé la décision du

---

[326] Dimitrios ZISSIS et Dimitrios LEKKAS, « Securing e-Government and e-Voting with an Open Cloud Computing Architecture », (2011) 28 *Government Information Quarterly* 239, 242.

[327] *Id*.

[328] Eric A. FISCHER et Patricia MOLONEY FIGLIOLA, « Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management », (2013). en ligne : < http://www.fas.org/sgp/crs/misc/R42887.pdf >

[329] Doug BEIZER, « USA.gov will move to cloud computing », (2009), en ligne : < http://fcw.com/articles/2009/02/23/usagov-moves-to-the-cloud.aspx >; Scott PAQUETTE, Paul T. JAEGER et Susan C. WILSON, « Identifying the Security Risks Associated with Governmental Use of Cloud Computing », (2010) 27 *Government Information Quarterly* 245, 247.

[330] S. PAQUETTE, P. T. JAEGER et S. C. WILSON, préc., note 329, 247. Par exemple, le *National Institute of Standards and Technology* (NIST) a lancé une chaîne sur YouTube le 19 décembre 2008 pour offrir une bibliothèque de conférences et de formations.

[331] Alice LIPOWICZ, « Living NOAA's Second Life », (2009), en ligne : < http://fcw.com/Articles/2009/03/23/Eric-Hackathorn-NOAA.aspx >. Par exemple, le *Air Force* a déployé *MyBase* en décembre 2008, une plate-forme virtuelle 3-D de recrutement et de formation. Voir Colleen O'HARA, « Virtual learning gets second wind from Second Life », (2009), en ligne : < http://fcw.com/articles/2009/05/04/feature-virtual-learning.aspx >. Un autre exemple est l'utilisation de *Second Life* par le *Centers for Disease Control and Prevention* pour promouvoir leur mission de partager des alertes de santé en utilisant les avatars à travers la communauté en ligne. Voir Nedra KLINE WEINRICH, « The CDC's Second Life », (2006), en ligne : < http://blog.social-marketing.com/2006/11/cdcs-second-life.html >. Un dernier exemple est celui du monde virtuel créé par la *National Oceanic and Atmospheric Administration* (NOAA), qui permet à l'organisme de partager ses laboratoires, ses cours, ses discussions de recherche et ses espaces de conférence avec les étudiants, les citoyens, les décideurs et les scientifiques du monde entier. Voir Alice LIPOWICZ, « Living NOAA's Second Life », (2009), en ligne : < http://fcw.com/Articles/2009/03/23/Eric-Hackathorn-NOAA.aspx >.

gouvernement américain[332], tout comme la réduction significative du niveau de consommation mondiale d'énergie[333]. En effet, l'utilisation de ce type d'infrastructure permet aux institutions gouvernementales de se débarrasser de leurs propres solutions TI, lesquelles, bien qu'elles ne soient pas utilisées à leur pleine capacité, consomment beaucoup d'énergie. Ainsi, l'externalisation vers le nuage serait une option beaucoup plus écologique.

i) Contraintes juridiques

Les risques juridiques identifiés par le gouvernement américain sont similaires à ceux mis de l'avant par le gouvernement australien et le gouvernement britannique. En effet, une préoccupation majeure était la sécurité informationnelle du nuage et à sa capacité d'empêcher l'accès non autorisé aux données[334], ainsi que les attaques malveillantes[335]. De plus, le gouvernement américain était très préoccupé par la question de la conformité aux lois et règlements [336] relatifs aux exigences de sécurité propres à certains organismes gouvernementaux[337]. En effet, bien que le gouvernement américain ait migré vers le nuage, la nature même de cette infrastructure rend le respect de certaines lois impossible[338].

En outre, comme les gouvernements australien et britannique, le gouvernement américain exprime certaines inquiétudes au niveau de la fragmentation des données dans le nuage,

---

[332] Vivek KUNDRA, « Federal Cloud Computing Strategy », (2011), en ligne : < https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf >, p. 6.

[333] U.S. ENVIRONMENTAL PROTECTION AGENCY, « Report to Congress on Server and Data Center Energy Efficiency Public Law 109-431 », (2007), en ligne : < http://hightech.lbl.gov/documents/DATA_CENTERS/epa-datacenters.pdf >; E. A. FISCHER et P. MOLONEY FIGLIOLA, préc., note 328; ACCENTURE, « Cloud Computing and Sustainability : The Environmental Benefits of Moving to the Cloud », (2010), en ligne : < http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Sustainability_Cloud_Computing_TheEnvironmentalBenefitsofMovingtotheCloud.pdf >; Sophie CURTIS, « Forrester: The Cloud Is Inherently Green », (2011), en ligne : < http://www.techweekeurope.co.uk/news/forrester-the-cloud-is-inherently-green-33331 >.

[334] S. PAQUETTE, P. T. JAEGER et S. C. WILSON, préc., note 329, 252.

[335] Michael ARMHURST et al., « Above the Clouds: A Berkely View of Cloud Computing », (2009), en ligne : < http://www.cs.columbia.edu/~roxana/teaching/COMS-E6998-7-Fall-2011/papers/armbrust-tr09.pdf >.

[336] S. PAQUETTE, P. T. JAEGER et S. C. WILSON, préc., note 329, 250.

[337] E. A. FISCHER et P. MOLONEY FIGLIOLA, préc., note 328.

[338] Roy MARK, « Do Federal Agencies Belong in Cloud Computing Networks? », (2008), en ligne : < http://www.eweek.com/c/a/Government-IT/Should-Feds-Climb-on-the-Cloud/ >.

notamment parce que cette pratique augmente les risques d'accès non autorisés[339]. Le gouvernement américain a également manifesté des inquiétudes similaires à celles des gouvernements australien et britannique quant à la fiabilité[340] et à la disponibilité du nuage[341].

L'intégrité des données stockées dans le nuage est aussi une préoccupation importante pour le gouvernement américain. Comme nous le verrons plus loin[342], l'intégrité comprend un certain nombre d'éléments qui sont essentiels afin de prévenir ou d'atténuer les risques qui affectent l'exactitude des informations gérées[343]. Toute information stockée dans une infrastructure infonuagique doit maintenir son intégrité et sa précision dans son contexte pour avoir de la valeur pour le client. Le prestataire doit s'assurer de prendre toutes les précautions nécessaires pour garantir que les données stockées dans le nuage ne deviennent pas corrompues ou modifiées[344].

Au-delà de l'évaluation de l'intégrité des informations stockées dans le nuage, un élément intéressant de la vérification informatique est l'identification de la source d'information, la manière dont elle est utilisée par la suite, ainsi que l'identité des personnes qui l'utilisent. Dans les systèmes internes, une fois que les données sont supprimées à partir d'un serveur, il est difficile de les suivre jusqu'à leur nouvel emplacement. L'infonuagique peut atténuer ce problème en suivant le document et en incluant les métadonnées (comme les adresses IP) de son nouvel emplacement[345]. Par exemple, une étude récente a conclu que les données médicales sensibles hébergées dans le nuage pourraient être fusionnées avec d'autres bases de données et pourraient donc compromettre la confidentialité des données, en divulguant l'identité des patients et d'autres données électroniques[346]. On estime que le marché pour ces données médicales pourrait dépasser

---

[339] S. PAQUETTE, P. T. JAEGER et S. C. WILSON, préc., note 329, 249.

[340] *Id.*, 252.

[341] *Id*.

[342] *Infra*, pp. 90 et ss.

[343] S. PAQUETTE, P. T. JAEGER et S. C. WILSON, préc., note 329, 250.

[344] *Id.*

[345] *Id.*, 249.

[346] Au Canada, une problématique similaire a d'ailleurs été soulevée dans l'affaire *Gordon* c. *Canada (Santé)*, 2008 CF 258 en ce qui concerne le référencement croisé à l'intérieur de certaines bases de données médicales.

5 milliards de dollars, même si la vente de ces données serait illégale en vertu de la *Health Insurance Portability and Accountability Act*[347].

Le gouvernement américain a également soulevé certaines inquiétudes quant au niveau de protection des droits de propriété intellectuelle des données stockées dans le nuage (nous y reviendrons), ainsi qu'au niveau du contrôle des données qui sont crées et modifiées à l'aide des services infonuagiques[348]. En raison d'un manque de politiques fédérales et d'un manque de précédents jurisprudentiels, il n'est pas clair qui possède les informations (et leurs métadonnées) une fois qu'elles sont hébergées dans le nuage.

ii) Solution retenue

Bien que plusieurs risques soient associés au recours à l'infonuagique par les agences gouvernementales, l'utilisation d'infrastructure technologique par le gouvernement est stratégique, à condition qu'« un programme de gestion de risques prudent [soit] développé pour éviter des conséquences technologiques non désirées »[349]. Pour accomplir cela, le gouvernement américain compte créer un environnement de sécurité transparent entre les prestataires de services infonuagiques et les consommateurs. Cet environnement permettra au gouvernement états-unien d'évaluer le niveau de sécurité d'une manière plus compréhensive que ce qui est actuellement prévu au sein des organismes. La première étape de ce processus fut le *Federal Risk and Authorization Management Program* (FedRAMP) de 2010. FedRAMP définit les exigences pour les contrôles de sécurité dans le nuage, y compris l'analyse de vulnérabilité, le suivi des incidents, la connexion et le rapportage[350]. La mise en œuvre de ces contrôles améliorera et encouragera la confiance dans l'environnement infonuagique. Pour renforcer la sécurité d'un point de vue opérationnel, le *Department of Homeland Security* priorisera une liste des principales

[347] Kim ZETTER, « Medical Records : Stored in the Cloud, Sold on the Open Market », (2009), en ligne : < http://www.wired.com/threatlevel/2009/10/medicalrecords >.

[348] S. PAQUETTE, P. T. JAEGER et S. C. WILSON, préc., note 329, 252.

[349] *Id.*, 245.

[350] Voir : U.S. GENERAL SERVICES ADMINISTRATION, « FedRAMP : Ensuring secure cloud computing for the Federal Government », en ligne : < http://www.gsa.gov/portal/category/102371?utm_source=OCSIT&utm_medium=print-radio&utm_term=fedramp&utm_campaign=shortcuts >.

menaces de sécurité tous les six mois ou au besoin et travaillera avec une équipe d'experts en sécurité au niveau gouvernemental pour s'assurer que les contrôles et les mesures de sécurité adéquates soient mis en œuvre. NIST publiera des lignes directrices de sécurité technique, comme celles axées sur la surveillance continue de solutions d'infonuagique, en conformité avec le cadre de gestion des risques en six étapes[351].

Les normes seront déterminantes pour l'adoption et la livraison des services infonuagiques, tant dans le secteur public que dans d'autres domaines. Les normes sont essentielles afin de s'assurer que les nuages ont une plateforme interopérable pour que les services fournis par différents prestataires puissent être mis en commun, peu importe si ces services sont fournis à l'aide d'un modèle public, privé, communautaire ou hybride[352].

Le NIST jouera un rôle central en définissant les normes et en collaborant avec les directeurs des systèmes d'information des agences, des experts du secteur privé et des organismes internationaux pour identifier, hiérarchiser et parvenir à un consensus quant aux priorités de normalisation. En 2010, le NIST a organisé des ateliers de mobilisation pour identifier et prioriser les besoins. Dorénavant, le NIST va générer, évaluer et réviser un plan infonuagique périodiquement. Ce plan suivra et définira les priorités convenues afin de coordonner les efforts entre les parties prenantes[353].

Le NIST conservera un rôle de leadership en donnant priorité au développement, à l'évolution et à l'amélioration de normes au fil du temps[354]. Il collaborera avec les organismes afin de définir un ensemble de cas cibles d'utilisation d'affaires qui posent les plus grands défis à la lumière des risques, des préoccupations ou des contraintes qui sont associés à ces cas.

Le NIST continuera à exécuter le projet du *Standards Acceleration to Jumpstart Adoption of Cloud Computing* (« SAJACC »), qui joue un rôle important dans la validation des spécifications

[351] V. KUNDRA, préc., note 332, p. 26.

[352] *Id.*, p. 29.

[353] *Id.*

[354] *Id.*

clés des nuages et dans le partage de l'information, afin de renforcer la confiance dans les technologies infonuagiques avant que les normes officielles soient disponibles. À ce jour, la SAJACC a défini 24 cas d'utilisations techniques génériques qui peuvent être utilisés pour valider l'interopérabilité, la sécurité et les exigences de portabilité[355].

[355] *Id.*, p. 30.

SECTION II : Les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec

Si la première partie de la présente étude nous aura permis d'identifier les caractéristiques de l'infonuagique, ainsi que les avantages et inconvénients en découlant, il demeure que les particularités du contexte québécois viendront baliser les possibilités offertes à l'administration gouvernementale dans le domaine. En effet, si le recours à l'infonuagique semble, à bien des égards, bénéfique pour l'état québécois, il demeure que le cadre juridique applicable viendra en quelque sorte limiter les types de modèles de déploiement et de service envisageables. Nous tenterons donc, dans la présente section, de cerner les principes et balises imposés par ce cadre législatif (A), pour ensuite tenter d'en identifier les incidences par le biais d'analyses de cas concrets (B).

A. Le cadre juridique applicable à l'utilisation de l'infonuagique par le gouvernement du Québec : principes et balises

Tel que nous l'avons identifié en première partie, l'infonuagique implique la délocalisation, dans le nuage, de divers services et contenus informatiques, qu'il s'agisse de données, d'applications logicielles, de plateformes, voire même d'infrastructures informatiques. Si, du point de vue technologique, ces services et contenus offrent des fonctionnalités et servent à des fins distinctes, leur cadre juridique repose sur des principes communs. Ainsi, une majorité de contenus ou d'applications accessibles via le nuage pourront être qualifiés de « documents technologiques ». Rappelons que, en vertu de la *Loi concernant le cadre juridique des technologies de l'information* (ci-après : la *LCCJTI*), un document est constitué d'informations portées par un support faisant appel à une technologie donnée[356]. Si ce support fait appel aux technologies de l'information, comme ce serait nécessairement le cas en matière d'infonuagique, alors le document sera qualifié de « document technologique ». Plus précisément, un document

[356] Notons ici que le terme technologie est utilisé au sens large.

technologique sera constitué d'informations délimitées et structurées de façon logique et portées par un support faisant appel aux technologies de l'information[357].

DOCUMENT = INFORMATION + SUPPORT

DOCUMENT TECHNOLOGIQUE = INFORMATION + SUPPORT FAISANT APPEL AUX TI

En effet, les logiciels, au même titre que les données de citoyens, ne sont rien de plus que de l'information emmagasinée sur un support, en l'occurrence les serveurs composant le nuage d'un prestataire de service d'infonuagique. Toutefois, si ces données, logiciels et autres applications constituent tous des documents technologiques aux yeux du législateur, il demeure que les obligations juridiques découlant de l'hébergement de ces documents dans le nuage varieront selon le type de document visé.

L'administration gouvernementale doit donc tenir compte des types de documents technologiques qui pourraient se retrouver dans le nuage et des risques associés à un tel hébergement décentralisé (lesquels varieront selon le modèle de déploiement choisi). Ainsi, nous verrons que les ministères et organismes publics québécois se devront, selon le cas, de respecter les exigences imposées par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[358] (ci-après : la « *Loi sur l'accès* »), la *LCCJTI* et les lois sectorielles qui s'appliquent aux types de documents technologiques qui pourraient se retrouver dans le nuage.

Selon Peter S. Browne, les risques associés à l'hébergement de données ou, plus exactement, aux données elles-mêmes (qu'elles soient contenues dans un document technologique ou tout autre type de document) peuvent être résumés comme suit : [traduction] « les données peuvent être divulguées, détruites ou modifiées, soit accidentellement, soit volontairement »[359]. L'organisme public désirant héberger des données dans le nuage devra donc s'assurer de mettre en place les

[357] *LCCJTI*, art. 3.

[358] RLRQ, c A-2.1.

[359] P. S. BROWNE, préc., note 24.

mesures de sécurité pour **limiter** ces risques[360], c'est-à-dire « prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[361] (notre soulignement).

Or, dès lors qu'il est admis que certains documents technologiques voués à être hébergés dans le nuage nécessitent que l'on en assure la sécurité, il importe d'établir comment cette obligation doit être traduite juridiquement. En effet, la sécurité est en soi un concept fourretout tributaire d'une panoplie de caractéristiques propres aux données[362]. Toutefois, parmi ces caractéristiques, trois retiennent notre attention : la disponibilité, l'intégrité et la confidentialité de l'information. Ces trois caractéristiques, représentées conjointement par certains auteurs sous l'appellation « Triade CID ou DIC »[363], constituent – selon la position dominante – les piliers de la sécurité de l'information[364]. Elles sont par ailleurs citées dans la *Directive sur la sécurité de l'information gouvernementale* comme étant nécessaire afin de « maintenir et de rehausser la confiance à l'égard de l'État et des services publics qu'il rend »[365].

Le législateur, à l'article 26 de la *LCCJTI* (lequel sera analysé plus loin), semble également avoir adopté cette position dominante en prévoyant l'obligation pour le gardien de l'information – en l'occurrence le prestataire de services infonuagiques – de « préserver l'intégrité [de l'information]

---

[360] Rappelons, en effet, que le risque zéro n'existe pas. Il n'est donc pas envisageable d'éliminer les risques, seulement de les réduire à un niveau jugé raisonnable. Pour une analyse approfondie de cette obligation, voir N. W. VERMEYS, préc., note 129.

[361] *Loi sur l'accès*, art. 63.1.

[362] Éric LACHAPELLE et René ST-GERMAIN, « Protection des actifs informationnels », dans Abdelhaq ELBEKKALI, *Gouvernance, audit et sécurité des TI*, Brossard, CCH, 2008, p. 315, à la page 351.

[363] Voir N. W. VERMEYS, préc., note 129, p. 24.

[364] *Id.*, p. 23 et ss.

[365] SERVICES GOUVERNEMENTAUX QUÉBEC, « Directive sur la sécurité de l'information gouvernementale », 2006, Québec, p. 2. Notons que cette directive ajoute l'identité et la non-répudiation à la liste des caractéristiques devant être assurées. Nous n'aborderons toutefois pas ces deux critères supplémentaires dans le cadre de la présente étude d'abord parce qu'ils ont été écartés par le législateur, ensuite parce que, tel que nous l'avons écrit ailleurs, nous considérons qu'une interprétation large de la triade DIC vient incorporer ces critères. Voir N. W. VERMEYS, préc., note 129, p. 31 et ss.

et, le cas échéant, [d']en protéger la confidentialité et [d']en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance ». Ainsi, tout ministère ou organisme public québécois se voit dans l'obligation d'assurer la disponibilité (1), l'intégrité (2) et la confidentialité (3) des documents technologiques qu'il détient, même lorsqu'il en confie la conservation à un tiers[366]. Ce sont donc ces trois caractéristiques qui feront l'objet de la prochaine section de la présente étude.

1) La disponibilité des documents technologiques

Définition :	Propriété d'un document qui est accessible dans les délais convenables pour les personnes autorisées.
Documents visés :	Tout document technologique contenant ou permettant d'avoir accès à une information.
Modèles de déploiement à favoriser :	• Modèle privé interne ou communautaire. • Tout autre modèle si des copies de sauvegarde de l'information et des logiciels sont gardées sur les serveurs de l'organisme public.

Le principe de la disponibilité de l'information implique que les documents détenus par un organisme public se doivent d'être « accessibles dans les délais convenables pour les personnes autorisées à en disposer dès qu'elles le désirent »[367], d'abord pour des raisons juridiques[368], ensuite parce qu'un document qui n'est pas disponible pour l'organisme public (ou tout au moins certains de ses dirigeants et/ou des membres de son personnel, voire même des citoyens) s'avère inutile. Or, comme nous l'avons souligné en introduction de la présente sous-section, un document technologique est composé d'informations portées par un support faisant appel à une technologie. Ainsi, la disponibilité du document dépendra ultimement de ces deux composantes. En d'autres mots, l'obligation d'assurer la disponibilité de documents technologiques visera tant la disponibilité des données (a) que de l'infrastructure informatique et logicielle (b).

[366] En effet, rappelons que, en vertu de l'article 1er de la *Loi sur l'accès*, même lorsqu'un organisme public confie la conservation d'un document à un tiers, il en conserve la détention juridique. Voir Raymond DORAY et François CHARETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Yvon Blais, 2001, p. I/1-1 et ss. Voir également *Office du crédit agricole du Québec* c. *Boucher*, (c.p.) [1987] C.A.I., 252, 254.

[367] Joël HUBIN et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur, Crid, 1998, p. 7.

[368] Comme nous le verrons, cette obligation est prévue par différentes dispositions, dont les articles 9 et 83 de la *Loi sur l'accès*.

L'hébergement dans le nuage doit donc tenir compte de cette réalité et ne pas entraver l'accès légitime à ces composantes, tout en limitant l'accès des tiers[369].

a) La disponibilité des données

Avant même d'aborder la question de la disponibilité des données, une précision terminologique s'impose. En effet, comme nous venons de le souligner, la disponibilité est définie comme étant la « [p]ropriété d'une information ou d'une ressource informationnelle d'être accessible en temps voulu et de la manière requise par une personne autorisée »[370]. Il ne faut donc pas confondre l'obligation d'assurer la disponibilité de données et l'obligation d'y donner un accès au sens de la *Loi sur l'accès*. En effet, si la disponibilité est nécessaire pour permettre à un citoyen de profiter de son droit d'accès à l'information (au sens de l'article 9 de la *Loi sur l'accès*), elle ne se limite pas à ce seul contexte. Ainsi, l'obligation d'assurer la disponibilité de données visera également et surtout la possibilité pour un représentant d'un organisme ou d'un ministère d'avoir accès en temps opportun aux documents qu'il doit consulter pour effectuer ses tâches.

Peu importe le modèle de service d'infonuagique utilisé par un organisme public, le nuage, comme tout support technologique, vise ultimement à faciliter le traitement de données. Comme nous le verrons plus en détails dans la sous-section portant sur la confidentialité des documents technologiques, ces données auront soit un caractère public (débats parlementaires, informations aux citoyens), soit un caractère privé (renseignements personnels et confidentiels), dans quel cas leur disponibilité devra être contrôlée tant au niveau des accès autorisés[371], que par rapport au cycle de vie du document[372]. En effet, il importe de préciser que la disponibilité d'une

---

[369] *LCCJTI*, art. 26.

[370] GOUVERNMENT DU QUÉBEC, « Guide relatif à la catégorisation des documents technologiques en matière de sécurité », Québec, 2003, p. 4. Voir également Harold F. TIPTON et Micki KRAUSE, *Information Security Management Handbook*, 6e éd., Boca Raton, Auerbach Publications, 2007, p. 3020.

[371] En effet, le 1er alinéa de l'article 62 de la *Loi sur l'accès* prévoit que : « Un renseignement personnel est accessible, sans le consentement de la personne concernée, à toute personne qui a qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de ses fonctions ». Par ailleurs, comme nous l'avons vu l'article 26 de la *LCCJTI* oblige le prestataire de services infonuagiques à « interdire l'accès à toute personne qui n'est pas habilitée à […] prendre connaissance » d'un document technologique.

[372] La notion de cycle de vie d'un document est prévue au second alinéa de l'article 6 de la *LCCJTI*, lequel indique que : « L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant

information doit être limitée dans le temps, comme le souligne d'ailleurs l'article 73 de la *Loi sur l'accès* : « [l]orsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire »[373].

Ainsi, il est à supposer que, si une information a été recueillie par un organisme public et que cet organisme détient toujours cette même information, c'est qu'elle lui est utile selon les fins pour lesquelles elle a été recueillie et, donc, qu'elle se doit d'être disponible pour les personnes concernées. En d'autres mots, les renseignements hébergés dans le nuage par un organisme public devraient normalement constituer des informations auxquelles il est important, pour cet organisme, d'avoir accès afin qu'il puisse offrir les services au cœur de son mandat ou nécessaires à l'application d'une loi.

Toutefois, comme nous y avons fait référence précédemment, les employés de l'organisme public ne sont pas les seuls à pouvoir avoir accès à certains des renseignements qu'ils pourraient choisir d'héberger dans le nuage et donc pour qui ces renseignements se doivent d'être disponibles. En effet, en vertu de l'article 9 de la *Loi sur l'accès*, « [t]oute personne qui en fait la demande a droit d'accès aux documents d'un organisme public ». Évidemment, ce droit d'accès ne visera pas les renseignements confidentiels détenus par l'organisme public, mais si de tels renseignements se retrouvent à l'intérieur d'un document sans en former la substance, l'organisme se devra de « donner accès au document demandé après en avoir extrait uniquement les renseignements auxquels l'accès n'est pas autorisé »[374]. De plus, l'article 10 de la *Loi sur l'accès* prévoit que « [l]e droit d'accès à un document s'exerce par consultation sur place pendant les heures habituelles de travail ou à distance ». L'accès sur place, s'il est bien encadré, s'avère peu problématique. Par contre, permettre l'accès à distance à un citoyen implique la mise en place de balises l'empêchant d'accéder à toute autre donnée hébergée dans le nuage, notamment aux informations caviardées.

---

par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction ».

[373] « Sous réserve de la *Loi sur les archives* (chapitre A-21.1) ou du *Code des professions* (chapitre C-26) ». *Loi sur l'accès*, art. 73.

[374] *Loi sur l'accès*, art. 14.

La personne concernée par un renseignement personnel aura également, selon le type de dossier, un droit d'accès auxdits renseignements[375]. Ainsi, les accès accordés à l'information disponible dans le nuage devront tenir compte de restrictions particulières propres à certains types de documents ou de dossiers[376]. L'architecture des outils de consultation devra donc être développée afin de respecter ces restrictions.

Comme pour l'accès général aux documents des organismes publics, l'accès de la personne concernée par un renseignement personnel peut se faire a distance[377], nécessitant donc l'obtention de codes d'accès et, si l'information est chiffrée, d'outils permettant de rendre l'information lisible[378]. En effet, comme nous le verrons dans la section sur la confidentialité, l'obligation de sécurité associée à l'hébergement dans le nuage de renseignements confidentiels imposera, notamment lorsque les serveurs du prestataire de services infonuagiques sont situés à l'extérieur du Canada, de chiffrer certaines données, c'est-à-dire de les « [t]ransformer […] en un cryptogramme, de manière à [les] rendre inintelligible[s] à toute personne non autorisée et à en assurer ainsi la confidentialité »[379]. Ainsi, si les données sont chiffrées, leur disponibilité sera affectée, d'où la nécessité de fournir les outils nécessaires pour déchiffrer lesdites données aux personnes possédant un droit d'accès en vertu de la loi.

b) La disponibilité des infrastructures

La disponibilité de l'information et les droits d'accès qui la rendent nécessaire ne pourront toutefois être assurés à moins que les infrastructures informatiques et logicielles où sont hébergées ces données ou encore qui permettent la lecture ou l'analyse de celles-ci soient elles-mêmes disponibles. En effet, le recours à l'infonuagique nécessitera la mise en place d'un plan de

---

[375] *Loi sur l'accès*, art. 83 et ss.; C.c.Q., art. 38. Voir également, en matière fiscale, l'article 69.0.0.2 de la *Loi sur l'administration fiscale*, L.R.Q. c. A-6.002.

[376] Par exemple, l'article 64 de la *Loi sur l'assurance maladie*, RLRQ, c. A-29 et l'article 17 de la *Loi sur les services de santé et les services sociaux*, RLRQ, c. S-4.2, imposent certaines limites aux droits d'accès relatifs à des informations liées à des services de santé.

[377] *Loi sur l'accès*, art. 84.

[378] *Id.*

[379] OLF, préc., note 3.

continuité des activités[380] advenant une panne des serveurs ou une perte de connexion au réseau local, voire même à Internet. Au-delà de l'obligation générale imposée aux organismes publics de rendre des services aux citoyens, un tel plan se veut nécessaire notamment en vertu de l'article 19 de la *LCCJTI*, lequel prévoit que : « [t]oute personne doit, pendant la période où elle est tenue de conserver un document […] voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné ». Cette disposition doit être lue conjointement avec l'article 23 de la même loi, lequel précise notamment que : « [t]out document auquel une personne a droit d'accès doit être intelligible, soit directement, soit en faisant appel aux technologies de l'information ». En effet, même si les données visant un citoyen sont hébergées sur les serveurs de l'organisme, celles-ci s'avèrent inutiles si elles nécessitent le recours à une application hébergée dans le nuage à laquelle il ne peut avoir accès parce que la disponibilité de cette application a été compromise.

Il importe toutefois de souligner que, en matière d'infonuagique, la principale problématique liée à la disponibilité des données découlera du fait que l'accès est contrôlé par un tiers qui pourrait – volontairement ou par erreur – retirer des permissions ou des droits d'accès, voire même retenir des données pour faute de paiement ou toute autre raison qu'il considère légitime. Aux États-Unis, des prestataires de services d'hébergement se sont même déclarés propriétaires de dossiers publics, notamment de dossiers judiciaires[381]. Ainsi, l'organisme public dont le prestataire de services infonuagiques interdirait l'accès aux renseignements hébergés, en plus de ne pas pouvoir lui-même exploiter ces renseignements pour les fins pour lesquelles ils ont été recueillis, s'exposerait à des poursuites de la part de citoyens ne pouvant exercer leur droit d'accès. Évidemment, il est possible de limiter contractuellement les risques liés à un tel abus de pouvoir de la part du prestataire de services infonuagiques, mais, si ce dernier ne respecte pas les conditions du contrat, les délais entre la perte de disponibilité et l'obtention d'un jugement forçant l'accès demeurent inquiétants. Notons que la même problématique existe si, comme nous

[380] « Plan visant à assurer le rétablissement en temps opportun ou la disponibilité continue des fonctions et services opérationnels de l'entreprise dans l'éventualité où les ressources habituelles, comme les bureaux, les terminaux, les micro-ordinateurs et les réseaux, cesseraient d'être disponibles ». Voir OLF, préc., note 3.

[381] Voir notamment Kevin M. OEFFNER, « e-Filing Update », (2006), en ligne : < http://www.oakgov.com/courts/circuit/Documents/laches/june-06-laches-c.pdf >.

l'avons vu dans la première partie de la présente étude, l'accès au nuage est interrompu parce que l'infrastructure du prestataire de services infonuagiques n'est pas suffisamment robuste pour satisfaire au nombre de demandes ou est exposée à des pannes électriques récurrentes ou prolongées. Le choix du prestataire de services infonuagiques devra donc tenir compte de ces risques[382].

Pour éviter de se trouver dans une situation où la disponibilité de l'information serait compromise, l'organisme public pourra choisir soit de recourir à un modèle d'infonuagique privé interne, soit de garder une copie des documents sur ses propres serveurs. Évidemment, dans ce dernier cas, un tel dédoublement de l'information viendra en quelque sorte neutraliser les avantages procurés par l'infonuagique. Qui plus est, la multiplication des copies pourrait entraîner une multiplication des versions d'un même document et, de ce fait, complexifier le travail des employés de l'organisme, lesquels ne sauront plus à quelle version d'un document se fier, augmentant ainsi les risques d'erreurs et de mauvaises informations.

2) L'intégrité des documents technologiques

Définition :	Propriété d'un document dont l'information n'est pas altérée et est maintenue dans son intégralité.
Documents visés :	Tout document technologique (mais principalement 1- celui contenant des informations qui servent à une prise de décision; 2- celui qui pourrait être soumis en preuve devant les tribunaux; ou 3- celui pour lequel la loi impose la mise en place de mesures en assurant l'intégrité).
Modèles de déploiement à favoriser :	• Tout modèle de déploiement dès lors que l'infrastructure en place permet d'assurer l'intégrité tant des documents technologiques que des métadonnées y associées.

L'intégrité est une « [p]ropriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation »[383]. Joël Hubin et Yves Poullet proposent une définition similaire : « [l]a propriété d'être conservé intact, sans dommage et sans perte, et de

[382] Sur ce point, voir J. RHOTON, J. De CLERC et D. GRAVES, préc., note 32, p. 250.

[383] OLF, préc., note 3.

n'être détruit ou transformé que par l'intervention des personnes autorisées à le faire »[384]. Les mêmes auteurs poursuivent en précisant que « [l]'intégrité peut être répartie en deux qualités qui sont l'authenticité du contenu et l'authenticité de l'origine »[385].

Législativement, ce même concept est défini de la façon suivante à l'article 6 de la *LCCJTI* :

> « [l]'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue. »[386]

Un document dont l'intégrité est compromise deviendra, dans biens des cas, inutile. C'est pourquoi l'article 6 de la *LCCJTI* prévoit également que « [l]'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction », alors que l'article 19 de la même loi précise que « [t]oute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné ».

Notons que si ces dispositions visent principalement le droit de la preuve[387], elles ne devraient pas être interprétées comme s'y limitant. En effet, le ministère ou l'organisme public qui prend une décision en se basant sur une information dont l'intégrité a été atteinte pourrait causer un préjudice à un citoyen ou un groupe de citoyens donné et, donc, s'exposer à une poursuite en

---

[384] J. HUBIN et Y. POULLET, préc., note 367, p. 7.

[385] *Id*. Notons toutefois que cette adéquation entre les notions d'intégrité et d'authenticité est parfois source de confusion et ne fait pas nécessairement l'unanimité. Voir Claude FABIEN, « La preuve par document électronique », (2004) 38 *R.J.T.* 533, 583.

[386] *LCCJTI*, art. 6. Cette définition est par ailleurs pratiquement identique à celle proposée au premier alinéa de l'article 2839 C.c.Q. : « L'intégrité d'un document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue ».

[387] D'ailleurs, plusieurs dispositions relatives à l'intégrité des documents dans la *LCCJTI* ont été reproduites dans le livre 7 du *Code civil*, lequel est intitulé « De la preuve ». Sur la question de l'intégrité en droit de la preuve, voir : Vincent GAUTRAIS, *Preuve technologique*, Montréal, Lexis Nexis, 2014, partie 2, chapitre 2, section 1 : « De l'intégrité ».

responsabilité civile. Au même titre que le document contenant des informations « inexactes, incomplètes ou équivoques »[388], un document dont l'intégrité n'est pas assurée n'est pas suffisamment fiable pour permettre une prise de décision. L'obligation d'assurer l'intégrité d'un document dépasse donc la simple préoccupation associée à son admissibilité en preuve devant les tribunaux judiciaires.

Comme les documents technologiques versés dans le nuage sont, comme nous l'avons vu, conservés par le prestataire de services infonuagiques, c'est à ce dernier que reviendra l'obligation d'assurer le maintien de l'intégrité des informations qu'ils contiennent. Évidemment, comme cette conservation lui aura été déléguée par l'organisme public, celui-ci sera ultimement responsable des dommages causés par une conservation lacunaire[389].

La principale problématique liée à l'intégrité des documents technologiques découlant du recours à l'infonuagique est liée à la structure du nuage. Tel que nous l'avons abordé en première partie, l'infonuagique est notamment caractérisée par le recours à une série « de serveurs distants interconnectés »[390]. Si cette structure offre une certaine flexibilité au nuage, elle implique par ailleurs qu'un document technologique pourrait se retrouver fractionné; chacune des parties étant alors hébergée sur un serveur distinct.

Le fait de fractionner un document technologique pour en héberger les fragments sur différents serveurs pourrait porter atteinte à l'intégrité des informations y contenues. Notons que cette fragmentation n'est pas – à notre avis – en soi suffisante pour prétendre à la perte d'intégrité du document. En effet, la *LCCJTI* prévoit que : « Le seul fait que le document ait été fragmenté, compressé ou remisé en cours de transmission pour un temps limité afin de la rendre plus efficace n'emporte pas la conclusion qu'il y a atteinte à l'intégrité du document »[391].

---

[388] *Loi sur l'accès*, art. 89. Voir également Cynthia CHASSIGNEUX, *Vie privée et commerce électronique*, Montréal, Thémis, 2004, p. 169 et ss.

[389] *LCCJTI*, art. 25.

[390] OLF, préc., note 3.

[391] *Id.*, art. 30.

Bien que cette disposition vise la transmission et non l'hébergement des données, nous sommes d'avis que la logique derrière celle-ci est transposable *mutatis mutandis* aux données hébergées dans le nuage. D'ailleurs, la *LCCJTI* prévoit également qu'une banque de données « dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite » est assimilée à un document aux fins de la loi[392].

Ainsi, si les risques pour l'intégrité ne découlent pas directement du fractionnement des données, ils en découlent indirectement. En effet, tel que nous l'avons abordé sous la rubrique « disponibilité de l'information », il est possible que l'un ou l'autre des serveurs qui composent le nuage devienne inaccessible. Qui plus est : [traduction] « les implémentations actuelles d'infonuagique présentent normalement un nombre d'erreurs plus élevé sur les plateformes virtuelles que ce à quoi nous pourrions nous attendre sur des appareils physiques »[393]. Or, si un document est fractionné en dix parties – chacune étant hébergée sur un serveur différent – et que chaque serveur a, par exemple, une chance sur cent d'être inaccessible, cela implique qu'un document hébergé dans ce nuage fictif aurait 10 % de chance de ne pas pouvoir être reconstitué et, donc, de perdre son intégrité, alors que les risques tomberaient à 1 % si ce même document était hébergé sur un serveur unique. Cet exemple (lequel, nous l'admettons, est très peu représentatif du fonctionnement réel des principaux services infonuagiques) vise principalement à démontrer la nécessité de prévoir des redondances[394] dans le système afin de s'assurer qu'un document fragmenté puisse toujours être reconstitué. Ainsi, l'organisme public désirant rencontrer ses obligations relatives à l'intégrité des documents qu'il détient devra s'assurer que les mesures de redondance adoptées par le prestataire de services infonuagiques sont suffisantes selon les types de données colligées et l'importance associée à leur intégrité.

---

[392] *LCCJTI*, art. 3.

[393] J. RHOTON, J. De CLERC et D. GRAVES, préc., note 32, p. 250.

[394] « Duplication d'un élément essentiel au fonctionnement normal du système informatique, en vue de pallier la défaillance éventuelle de cet élément et d'assurer ainsi la continuité d'une fonction informatique vitale. […] La redondance en sécurité informatique peut s'appliquer aussi bien à un centre informatique qu'à des éléments d'information, à des matériels, à des installations de sécurité, à des procédures et aux éléments vitaux d'une machine ». Voir OLF, préc., note 3.

Pour conclure cette sous-section, mentionnons que, lorsqu'un document est porté par un support technologique, son intégrité pourra notamment[395] être vérifiée par le biais de métadonnée, soit de « [d]onnée qui renseigne sur la nature de certaines autres données et qui permet ainsi leur utilisation pertinente »[396]. En effet, comme l'explique l'*Office de la langue française* :

> « Dans la perspective des entrepôts de données, les métadonnées sont un élément primordial et sont destinées à diverses catégories d'utilisateurs. Elles permettent notamment de connaître l'origine et la nature des données stockées dans l'entrepôt, de comprendre comment elles sont structurées, de savoir comment y avoir accès et comment les interpréter, de connaître les différents modèles de données en présence et les règles de gestion de ces données. »[397]

Ainsi, « [l]a preuve de l'intégrité du "document" se fera donc par la divulgation des métadonnées qui doivent être révélées sur le document et ce, indépendamment du type de support employé »[398]. Pour cette raison, l'obligation d'intégrité qui reviendra tant à l'organisme public qu'au prestataire de services infonuagiques à qui ont été confiés des documents technologiques ne se limitera pas au contenu de ces documents. Il visera également l'intégrité des métadonnées associées à ces documents[399] puisque, si les métadonnées ne sont pas intègres, il deviendra difficile d'établir l'intégrité des documents eux-mêmes et, donc, de prendre une décision éclairée en se basant sur ceux-ci.

---

[395] En effet, d'autres moyens de vérifier l'intégrité d'un document technologique sont prévus dans la *LCCJTI*, soit le recours à un procédé permettant d'établir que « la copie d'un document technologique [présente] des garanties suffisamment sérieuses pour établir le fait qu'elle comporte la même information que le document source » (*LCCJTI*, art. 15) – procédé qui pourrait lui-même impliquer la consultation des métadonnées, ou encore le recours à une documentation – notamment en cas de transfert de données (*LCCJTI*, art. 17) ou la transmission de documents (*LCCJTI*, art. 34).

[396] OLF, préc., note 3.

[397] *Id.*

[398] *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.*, 2013 QCCQ 1301, par. 51.

[399] *Richard* c. *Gougoux*, 2009 QCCS 2301, par. 77; *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.*, préc., note 398, par. 84.

3) La confidentialité des documents technologiques

Définition :	Propriété d'un document dont l'information ne peut être divulguée à une personne non autorisée.
Documents visés :	Tout document technologique contenant des renseignements confidentiels.
Modèles de déploiement à favoriser :	• Tout modèle de déploiement dès lors que les serveurs sont situés au Canada et que le prestataire est canadien. • Tout autre modèle de déploiement si les données sont chiffrées.

La confidentialité, soit la « [p]ropriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées »[400], constitue l'élément le plus couramment associé à la notion de sécurité. Nous n'avons qu'à penser aux différents ordres professionnels qui imposent le maintien du secret professionnel, ou aux innombrables technologies disponibles pour l'assurer. De ce fait, il s'agit également de l'élément le plus préoccupant pour les usagers du nuage. Pour cette raison, la présente section sera beaucoup plus détaillée que celles portant sur l'intégrité et la disponibilité des données. Nous désirons toutefois souligner que ce déséquilibre dans les parties est strictement lié à cette préoccupation et non à l'importance relative de l'une ou l'autre des composantes de la triade sécuritaire.

En droit, l'obligation de confidentialité est prévue par divers textes législatifs[401]. Toutefois, dès qu'une information confidentielle se retrouve à l'intérieur d'un document technologique, c'est l'article 25 de la *LCCJTI* qui vient établir les obligations du ministère ou de l'organisme responsable dudit document. En effet, cette disposition est à l'effet que :

> « [l]a personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non

[400] OLF, préc., note 3. Voir également J. HUBIN et Y. POULLET, préc., note 367, p. 7.

[401] Voir notamment les articles 67.2 et 125 de la *Loi sur l'accès*, l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P-39.1, les articles 19 et ss. de la *Loi sur les services de santé et les services sociaux*, etc. En fait, une recherche rapide sur le site du Canadian Legal Information Institute (www.canlii.org) nous permet de constater que la notion de confidentialité est prévue dans plus de 200 textes législatifs québécois, alors que le terme « confidentiel » se retrouve dans plus de 300 lois.

> autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder. »[402]

Il importe de souligner que cette disposition vise tout renseignement **confidentiel** et non le seul renseignement personnel. En effet, la notion de « renseignement confidentiel » ne saurait être réduite à celle de « renseignement personnel » puisque l'article 20 de la *LCCJTI* fait une distinction entre « renseignements confidentiels » et « renseignements personnels », démontrant ainsi que les deux termes ne sont pas synonymiques. D'ailleurs, comme l'explique Pierre-André Côté, en droit, « une variation dans l'expression signifie un changement dans les concepts signifiés »[403]. Il importe donc, avant toute chose, de définir ce qu'est un renseignement confidentiel (a), après quoi nous pourrons étudier plus en détail l'obligation de confidentialité liée à ces renseignements (b).

a) Les renseignements confidentiels

Notons d'emblée que l'expression « renseignement confidentiel », n'est pas fixée en droit québécois ou canadien[404]. En effet, outre certaines dispositions telles l'article 23 de la *Loi sur l'accès* (lequel énumère une série de types de renseignements qui pourraient être considérés confidentiels dans certains cas[405]), ou l'article 39 de la *Loi sur les télécommunications*[406] (lequel prévoit que peuvent être désignés comme des renseignements confidentiels : les secrets industriels, les renseignements financiers, commerciaux, scientifiques ou techniques qui sont de nature confidentielle et qui sont traités comme tels de façon constante par la personne qui les fournit, ou les renseignements dont la communication risquerait vraisemblablement soit de causer à une autre personne ou elle-même des pertes ou profits financiers appréciables ou de nuire à sa

---

[402] *LCCJTI*, art. 25.

[403] Pierre-André CÔTÉ, *Interprétation des lois*, 4e éd., Montréal, Thémis, 2009, p. 382.

[404] *R.* c. *Stewart*, [1988] 1 R.C.S. 963, par. 33.

[405] « Un organisme public ne peut communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement ». Notons que ce type de disposition se retrouve dans diverses autres lois québécoises. Par exemple, l'article 25 de la *Loi sur l'aquaculture commerciale*, RLRQ c. A-20.2 traite de « renseignements industriels, financiers, commerciaux, scientifiques ou techniques de nature confidentielle ».

[406] LC 1993, c. 38. Une énumération quasi-identique se retrouve également à l'article 20 (1) de la *Loi sur l'accès à l'information* (L.R.C. 1985, c. A-1).

compétitivité, soit d'entraver des négociations menées par cette autre personne ou elle-même en vue de contrats ou à d'autres fins), les textes législatifs demeurent quelque peu nébuleux quant à la portée à accorder à cette notion.

Selon la jurisprudence, « les renseignements sont confidentiels s'ils ne peuvent être obtenus de sources autrement accessibles au public ou si le simple membre du public agissant de son propre chef ne peut les obtenir par suite de ses propres observations ou études »[407]. Toutefois, l'utilité de cette définition demeure limitée puisqu'elle s'applique à l'obligation de divulgation de l'administration fédérale suite à une demande d'accès à l'information[408] et non à l'obligation de confidentialité imposée, notamment, par l'article 25 de la *LCCJTI*. Malgré ce fait, il découle de cette définition et des dispositions précitées que la notion de « renseignement confidentiel » peut être associée à celle de « secret industriel » (i). Toutefois, comme nous le verrons, elle vise également certains types de renseignements personnels (ii), ainsi que bon nombre d'autres renseignements qui, bien que normalement « publics », pourraient être jugés confidentiels selon le contexte de leur collecte ou de leur conservation (iii).

i) Les secrets industriels et autres renseignements connexes[409]

Tel que nous venons de le souligner, sont associés à des renseignements confidentiels les secrets industriels[410] ou commerciaux[411412], ainsi que certains renseignements financiers, commerciaux,

---

[407] *Air Atonabee Ltd. (f.a.s. City Express)* c. *Canada (Ministre des Transports)*, [1989] A.C.F. n° 453, par. 41; *Merck Frosst Canada Ltée* c. *Canada (Santé)*, 2012 CSC 3, par. 146.

[408] Voir *Merck Frosst Canada Ltée* c. *Canada (Santé)*, préc., note 407, par. 99.

[409] Pour une analyse exhaustive de ces différents types de renseignements, voir R. DORAY et F. CHARETTE, préc., note 366, p. II/23-1 et ss.

[410] La notion de secret industriel n'est pas définie en droit québécois (voir *Merck Frosst Canada Ltée* c. *Canada (Santé)*, préc., note 407, par. 105). Selon une publication de Santé Canada intitulée *Loi sur l'accès à l'information - Renseignements de tiers - Lignes directrices opérationnelles* (qui interprète donc la portée de cette notion au sens de la *Loi sur l'accès à l'information*), pour être qualifiée de secret industriel, une information « doit être secrète dans un sens absolu ou relatif (c'est-à-dire qu'elle est connue seulement d'une ou de quelques personnes); le détenteur de l'information doit démontrer qu'il a agi avec l'intention de traiter l'information comme si elle était secrète; l'information doit avoir une application pratique dans le secteur industriel ou commercial; le détenteur doit avoir un intérêt (par exemple, un intérêt économique) digne d'être protégé par la loi ». Voir *Astrazeneca Canada Inc.* c. *Canada (Ministre de la Santé)*, 2005 CF 189, par. 64 et 65. Voir également *Société Gamma Inc.* c. *Canada (Secrétariat d'État)*, [1994] A.C.F. n° 589, par. 7 et 8 et *Merck Frosst Canada Ltée* c. *Canada (Santé)*, préc., note 407, par. 109.

scientifiques ou techniques[413]. Cette association est d'ailleurs mise de l'avant par les tribunaux. Ainsi, dans l'affaire *Cadbury Schweppes Inc.* c. *Aliments FBI Ltée*[414], la Cour suprême propose de définir la notion de « renseignement confidentiel » comme suit :

> « Les renseignements, pour être confidentiels, doivent, me semble-t-il, indépendamment de tout contrat, posséder le caractère confidentiel nécessaire, c'est-à-dire qu'il ne doit pas s'agir de quelque chose qui appartient au domaine public et est de notoriété publique. En revanche, il est parfaitement possible qu'un document confidentiel, qu'il s'agisse d'une formule, d'un plan, d'un dessin ou de quelque chose du genre, soit le résultat du travail fait par son auteur à partir de matériaux accessibles à quiconque; ce qui le rend confidentiel est le fait que l'auteur du document s'est servi de son intelligence et a de la sorte obtenu un résultat que seul ce processus mental peut donner. »[415]

Soulignons finalement qu'une certaine position doctrinale favorise cette adéquation entre les notions de « secrets industriels » et de « renseignements confidentiels »[416]. Par exemple, l'honorable Marie-France Bich, avant d'être nommée à la Cour d'appel, a su indiquer que :

---

[411] « Information concernant des procédés de fabrication ou d'exploitation d'un produit que son bénéficiaire cherche à tenir confidentielle afin qu'elle ne soit pas divulguée à ses concurrents ». Hubert REID, *Dictionnaire de droit québécois et canadien*, 4e éd., Montréal, Wilson & Lafleur, 2010, p. 551. Pour une analyse jurisprudentielle de cette notion, voir : *R.L. Crain Limited* v. *R.W. Ashton & Ashton Press Mfg. Co. Ltd.*, [1949] 2 D.L.R. 481, par. 22 et ss. (confirmée en appel : [1950] 1 D.L.R. 601).

[412] Notons que, techniquement, les secrets industriels ne sont pas visés par l'expression « habituellement traité par un tiers de façon confidentielle » à l'article 23 de la *Loi sur l'accès*. Par contre, l'adéquation secret industriel – renseignement confidentiel a été réitérée à maintes reprises par les tribunaux, dont la Cour suprême. Voir *Merck Frosst Canada Ltée* c. *Canada (Santé)*, préc., note 407, par. 105.

[413] Voir, par exemple, l'article 23 de la *Loi sur l'accès* et l'article 25 de la *Loi sur l'aquaculture commerciale*.

[414] [1999] 1 RCS 142, par. 48.

[415] Ce passage est en fait un renvoi à la définition offerte dans *Saltman Engineering Co. v. Campbell Engineering Co.* (1948), 65 R.P.C. 203 (C.A.), à la p. 215, également reprise dans *Lac Minerals ltd.* c. *International Corona Resources ltd.*[1989] 2 RCS 574.

[416] F. Georges SAYEGH, *Les secrets de commerce et les renseignements confidentiels*, Cowansville, Yvon Blais, 2006, p. 1. L'auteur poursuit en précisant que les secrets de commerce et les renseignements confidentiels englobent une série de données et de documents tels : les ententes de partenariat, les contrats de coentreprise, les informations relatives à l'engagement ou au congédiement d'employés, les contrats d'achat ou de location, les contrats de franchise, les ententes de fusions ou d'acquisition (p. 2), ainsi que les informations « sur le marketing, la comptabilité, les ressources humaines et la masse salariale », des « composantes de la technologie de l'information » et des secrets de fabrication (p. 11). Une liste plus générique de la notion de « renseignement » reprenant la majorité de ces éléments tout en y ajoutant d'autres éléments qui pourraient constituer des renseignements confidentiels selon le contexte est fournie par l'auteur à la page 137 de cette même étude.

> « [s]ont habituellement considérés comme confidentiels les secrets de commerce ou de fabrication, les plans et maquettes liés au développement d'une technique ou d'un produit, les listes de clients secrètes ou contenant des renseignements privilégiés […] ou toute autre information qui n'est pas généralement connue et ne peut pas être obtenue ou reconstituée facilement. »[417].

Cela n'implique pas pour autant que ces types de renseignements sont nécessairement confidentiels. En effet, l'auteure poursuit en précisant que « [l]a qualification de "renseignements confidentiels" est une question de fait mais elle est aussi évaluée d'une façon objective. Il ne suffit pas que l'employeur décrète que tel ou tel renseignement est confidentiel pour qu'il le soit »[418]. Ces critères d'appréciation objective et subjective sont également soulevés et analysés par les auteurs Raymond Doray et François Charrette[419]. Comme l'expliquent ces derniers, la Commission d'accès à l'information a identifié quatre conditions qui doivent être satisfaites pour qu'un renseignement puisse être considéré confidentiel[420] :

- les renseignements doivent appartenir à l'une ou l'autre des catégories mentionnées à l'article 23 de la *Loi sur l'accès* (renseignement industriel, financier, commercial, scientifique, technique ou syndical);
- les renseignements doivent avoir été « fournis par un tiers » tel que précisé à ce même article 23;
- la nature confidentielle des renseignements doit être prouvée (critère objectif);

[417] Marie-France BICH, « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans *Développements récents en droit de la propriété intellectuelle*, Cowansville, Yvon Blais, 2003, p. 243, 305, telle que citée dans *Institut de zoothérapie du Québec Inc.* c. *Rioux*, 2005 CanLII 10507 (QC C.S.), par. 34. Voir également Sophie ROMPRÉ, *La surveillance de l'utilisation d'Internet au travail*, Cowansville, Yvon Blais, 2009, p. 31 : « Cette définition inclura généralement les secrets de commerce, secrets de fabrique, le savoir-faire et les autres informations stratégiques que détient l'entreprise ».

[418] Marie-France BICH, préc., note 417, p. 305. Pour une analyse plus complète de la notion de « renseignements confidentiels », voir Keith G. FAIRBAIRN et Julie A. THORBURN, *Law of Confidential Business Information*, Aurora, Canada Law Book, 2006, par. 3 :1000 et ss.

[419] R. DORAY et F. CHARETTE, préc., note 366, p. II/23-3 et II/23-4.

[420] *Id.*, p. II/23-3.

- les renseignements doivent habituellement être traités par le tiers de manière confidentielle (critère subjectif)[421].

Afin de fournir un éclairage supplémentaire, l'auteure Sophie Rompré[422] suggère que l'on s'inspire de la décision albertaine *Pharand Ski Corp.* c. *Alberta*[423], laquelle, se référant à deux décisions australiennes[424], offre une liste non exhaustive de critères permettant d'identifier le caractère confidentiel d'une information, à savoir :

- l'étendue de la diffusion de l'information à l'extérieur de l'entreprise;
- l'étendue de la diffusion de l'information au sein de l'entreprise;
- l'étendue des mesures de sécurité mise en place pour assurer la confidentialité de l'information;
- la valeur de l'information pour des tiers;
- l'argent et l'effort investis afin de collecter ou développer l'information;
- la facilité avec laquelle un tiers pourrait acquérir ou dupliquer l'information par lui-même[425].

Ainsi, en s'inspirant de ces diverses définitions et énumérations, toute information confiée à un organisme ou ministère par un tiers et ayant une valeur pour celui-ci pourra, selon le contexte, être qualifiée de renseignement confidentiel. Or, comme nous le verrons maintenant, ceci pourra également viser les renseignements personnels.

---

[421] *Id.* Voir également *Bourque* c. *Zangwill*, 2002 CanLII 9546 (QC CQ), par. 16; *Municipalité de Val-des-Monts* c. *Québec (Ministère du Développement durable, de l'Environnement et des Parcs)*, 2009 QCCAI 177, par. 31; et *M.R.* c. *Centre des services partagés du Québec*, 2010 QCCAI 3000, par. 88 et ss. Notons que ces quatre critères sont les mêmes que ceux employés par les tribunaux pour interpréter la portée de l'article 20(1) de la *Loi sur l'accès à l'information*. Voir : *Air Atonabee Ltd. (f.a.s. City Express)* c. *Canada (Ministre des Transports)*, préc., note 407, par. 33; *Astrazeneca Canada Inc.* c. *Canada (Ministre de la Santé)*, préc., note 410, par. 66.

[422] Sophie ROMPRÉ, préc., note 417, p. 31.

[423] 1991 CarswellAlta 85 (ABQB).

[424] *Ansell Rubber Co.* c. *Allied Rubber Industries Pty. Ltd.*, [1967] V.R. 37 et *Deta Nominees Pty. Ltd.* c. *Viscount Plastics Products Pty. Ltd.*, [1979] V.R. 167.

[425] *Pharand Ski Corp.* v. *Alberta*, préc., note 423, par. 144.

ii) Les renseignements personnels

Bien que la Cour suprême, dans l'affaire *Cadbury Schweppes Inc.* c. *Aliments FBI Ltée*[426] précitée, semble exclure les renseignements personnels de la notion de « renseignements confidentiels », cette exclusion ne saurait être acceptée au Québec puisque l'article 53 de la *Loi sur l'accès* prévoit expressément que « [l]es renseignements personnels sont confidentiels ». Ces renseignements, lorsque contenus dans un document technologique, seront donc visés par l'article 25 de la *LCCJTI* au même titre que les secrets industriels.

Rappelons que, en vertu de l'article 54 de la *Loi sur l'accès*, « sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier ». Une définition quasi identique est d'ailleurs offerte par le législateur dans la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après : la « *LPRPSP* »), à savoir : « [e]st un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier »[427].

Si la définition proposée est relativement large, elle fait l'objet de certaines exceptions. Ainsi, par exemple, le nom ou le prénom d'un citoyen, bien qu'il permette vraisemblablement d'identifier une personnel physique, ne saurait être considéré comme étant un renseignement personnel, « sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne »[428]. Ainsi, le nom d'un individu deviendra un renseignement personnel si, par exemple, il fait partie d'une liste de patients, ou de bénéficiaires d'un service donné[429].

Ensuite, bien qu'ils puissent être qualifiés de personnels, certains renseignements ne seront pas soumis « aux règles de protection des renseignements personnels » prévues par la *Loi sur*

[426] Préc., note 414, par. 48.

[427] *LPRPSP*, art. 2.

[428] *Loi sur l'accès*, art. 56.

[429] *GIFRIC inc.* c. *Corporation Sun Média (Journal de Québec)*, 2009 QCCA 236, par. 33 et ss.

l'accès[430], soit lorsque ces renseignements personnels auront un caractère public. Ces renseignements sont énumérés à l'article 57 de la *Loi sur l'accès* et visent :

- le nom, le titre, la fonction, la classification, le traitement, l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction et, dans le cas d'un ministère, d'un sous-ministre, de ses adjoints et de son personnel d'encadrement;

- le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public;

- un renseignement concernant une personne en sa qualité de partie à un contrat de services conclu avec un organisme public, ainsi que les conditions de ce contrat;

- le nom et l'adresse d'une personne qui bénéficie d'un avantage économique conféré par un organisme public en vertu d'un pouvoir discrétionnaire et tout renseignement sur la nature de cet avantage;

- le nom et l'adresse de l'établissement du titulaire d'un permis délivré par un organisme public et dont la détention est requise en vertu de la loi pour exercer une activité ou une profession ou pour exploiter un commerce.

Mentionnons toutefois que, toujours selon l'article 57 de la *Loi sur l'accès*, il existe en quelque sorte une exception à cette exception. Ainsi, les renseignements énumérés « n'ont pas un caractère public si leur divulgation est de nature à nuire ou à entraver le travail d'un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ». De plus, en ce qui concerne les renseignements « concernant une personne en sa qualité de partie à un contrat de services conclu avec un organisme public », ou les « nom et adresse d'une personne qui bénéficie d'un avantage économique conféré par un organisme public en vertu d'un pouvoir discrétionnaire », la confidentialité devra tout de même être assurée « dans la mesure où la communication de cette information révélerait un renseignement dont la communication doit ou peut être refusée en vertu de la section II du chapitre II » (restrictions au droit d'accès).

Finalement, soulignons que l'article 53 de la *Loi sur l'accès* prévoit que les renseignements personnels ne seront pas confidentiels si :

[430] *Loi sur l'accès*, art. 55.

- la personne concernée par ces renseignements consent à leur divulgation (si cette personne est mineure, le consentement peut également être donné par le titulaire de l'autorité parentale);

- ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle (ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion).

C'est donc dire que, au même titre que tous les renseignements confidentiels ne sont pas des renseignements personnels, tous les renseignements personnels ne sont pas, non plus, des renseignements confidentiels. D'ailleurs, l'article 55 de la *Loi sur l'accès* le prévoit expressément en soulignant qu'« un renseignement personnel qui a un caractère public en vertu de la loi n'est pas soumis aux règles de protection des renseignements personnels prévues par le présent chapitre », dont l'obligation de protection prévue à l'article 63.1.

Avant de conclure, il importe de rappeler que, indépendamment de l'article 25 de la *LCCJTI*, la confidentialité de renseignements personnels devra également être assurée en vertu de la *Loi sur l'accès*[431].

iii) Les autres renseignements

Outre les renseignements personnels ou autrement confidentiels, l'article 25 de la *LCCJTI* n'impose la protection d'aucun autre type de renseignement. Il en va de même, comme nous le verrons, pour la *Loi sur l'accès*. Ainsi, les organismes publics n'ont techniquement aucune obligation quant à la protection de renseignements ayant un caractère public[432], bien qu'ils doivent parfois, lorsque ces renseignements sont contenus dans un document technologique, limiter les fonctions de recherche associées à ce document[433].

---

[431] Voir notamment l'article 8 de la *Loi sur l'accès*.

[432] *Loi sur l'accès*, art. 55. Notons toutefois que, conformément au second alinéa de cet article, « un organisme public qui détient un fichier de tels renseignements peut en refuser l'accès, en tout ou en partie, ou n'en permettre que la consultation sur place si le responsable a des motifs raisonnables de croire que les renseignements seront utilisés à des fins illégitimes » (notre soulignement).

[433] *LCCJTI*, art. 24 : « L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière, est rendu public doit être restreinte à cette

Malgré ce fait, il importe de souligner que d'autres textes de loi considèrent que certains renseignements qui ne sont visés ni par l'article 53 (renseignement personnel), ni par l'article 23 (secret industriel, renseignement industriel, renseignement financier, renseignement commercial, renseignement scientifique, renseignement technique ou renseignement syndical) de la *Loi sur l'accès* doivent tout de même être considérés confidentiels. En effet, outre les renseignements confidentiels « par nature » visés par ces dispositions, certains renseignements qui seraient autrement considérés comme ayant un caractère public seront jugés confidentiels selon l'individu auquel ils auront été communiqués, selon le contexte de cette communication ou selon le contexte de leur conservation.

Ainsi, certains renseignements seront jugés comme étant confidentiels du seul fait qu'ils sont communiqués à un tiers auquel une obligation de confidentialité est imposée. C'est le cas, par exemple, de renseignements fournis à la Commission des droits de la personne :

> « Malgré les articles 9 et 83 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1), un renseignement ou un document fourni de plein gré à la Commission et détenu par celle-ci aux fins de l'élaboration, l'implantation ou l'observation d'un programme d'accès à l'égalité visé par la présente Charte ou par la *Loi sur l'accès à l'égalité en emploi dans des organismes publics* (chapitre A-2.01) est confidentiel et réservé exclusivement aux fins pour lesquelles il a été transmis; il ne peut être divulgué ni utilisé autrement, sauf du consentement de celui qui l'a fourni. »[434]

Dans d'autres cas, ce ne sera pas la personne à qui l'information est communiquée qui déterminera s'il s'agit d'un renseignement confidentiel, mais bien dans quel contexte une telle

---

finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés ».

[434] *Charte des droits et libertés de la personne*, RLRQ c. C-12, art. 93. Des exemples similaires existent notamment pour les renseignements sur l'origine d'un incendie obtenu par le ministre de l'assureur ou la municipalité (*Loi sur la sécurité incendie*, RLRQ c. S-3.4, art. 150); les échanges entre le directeur d'un établissement de détention et une victime (*Loi sur le système correctionnel du Québec*, RLRQ c. S-40.1, art. 175.1); les avis du jurisconsulte à un député (*Loi sur l'Assemblée nationale*, RLRQ c. A-23.1); les renseignements obtenus par un agent de surveillance de sentier (*Loi sur les véhicules hors route*, RLRQ c. V-1.2, art. 43); ou les renseignements confiés à un médiateur (*Loi sur les normes du travail*, RLRQ c. N-1.1, art. 123.3), un notaire (*Loi sur le notariat*, RLRQ c. N-3, art. 14.1), un acupuncteur (*Loi sur l'acupuncture*, RLRQ c. A-5.1, art. 13), la Commission des loyers (*Loi sur la Régie du logement*, RLRQ c. R-8.1, art. 91), ou un comptable agréé (*Loi sur les comptables agréés*, RLRQ c. C-48, art. 22.2).

information est communiquée. Ainsi, un renseignement recueilli dans le cadre d'une médiation[435], ou d'une conférence de règlement à l'amiable[436] sera confidentiel, tout comme un renseignement communiqué en vertu de la *Loi concernant les droits sur les mutations immobilières*[437], de la *Loi facilitant le paiement des pensions alimentaires*[438], de la *Loi sur l'impôt minier*[439], de la *Loi sur la protection de la jeunesse*[440], etc.[441].

Finalement, certains renseignements seront qualifiés de confidentiels du seul fait qu'ils se retrouvent dans un dossier dont le contenu est soumis à une obligation de confidentialité. C'est le cas, notamment, des renseignements contenus dans un dossier du tribunal de la jeunesse[442], un dossier administré par le curateur public[443], un dossier de l'Office des personnes handicapées du Québec concernant une personne handicapée[444], un dossier médical[445], ou un dossier fiscal[446].

Évidemment, dans une majorité des cas précités, le renseignement pourra être communiqué ou autrement partagé si la personne concernée par ces renseignements (ou le titulaire de l'autorité

[435] *Loi sur les chemins de fer*, RLRQ c. C-14.1, art. 19.

[436] *Code de procédure civile*, RLRQ c. C-25, art. 151.21.

[437] RLRQ c D-15.1, art. 22.

[438] RLRQ c. P-2.2, art. 75.

[439] RLRQ c. I-0.4, art. 80.2.

[440] RLRQ c. P-34.1, art. 72.5.

[441] C'est également le cas des renseignements concernant les conflits d'intérêts des administrateurs de la Caisse de dépôt communiqués au Ministre des Finances (*Loi sur la Caisse de dépôt et placement du Québec*, RLRQ c. C-2, art. 42); et des renseignements relatifs à un cotisant ou un bénéficiaire obtenus en vertu de la *Loi sur le Régime des rentes du Québec* (RLRQ c. R-9, art. 207).

[442] *Loi sur la protection de la jeunesse*, RLRQ c. P-34.1, art. 96.

[443] *Loi sur le Curateur public*, RLRQ c. C-81, art. 51.

[444] *Loi assurant l'exercice des droits des personnes handicapées en vue de leur intégration scolaire, professionnelle et sociale*, RLRQ c. E-20.1.

[445] *Loi sur les services de santé et les services sociaux pour les autochtones cris*, RLRQ c. S-5, art. 7; *Loi sur les services de santé et les services sociaux*, art. 19 ; *Loi sur l'Institut national de santé publique du Québec*, RLRQ, c. I-13.1.1, art. 34.

[446] *Loi sur l'administration fiscale*, art. 69.

parentale lorsque cette personne est un mineur) consent à sa divulgation[447], sur l'ordre d'un tribunal[448] ou dans tout autre cas prévu par la loi.

À la lumière de tout ce qui précède, nous sommes d'avis que, aux fins de la présente étude, doit être qualifié de « confidentiel » tout renseignement dont la loi interdit la divulgation volontaire ou involontaire à un tiers (à l'exception, dans certains cas, de la personne concernée) ou autorise la non-divulgation (notamment pour des fins de sécurité nationale). Cette définition sera celle que nous utiliserons pour la suite de notre analyse.

Bien que cela soit quelque peu extérieur à notre propos, nous nous en voudrions de ne pas soulever le fait que la protection de certains documents technologiques sera parfois nécessaire pour des intérêts commerciaux n'ayant aucun lien avec la confidentialité des données. En effet, certains documents, qu'ils contiennent ou non des renseignements confidentiels, ne sauraient être hébergés dans le nuage s'ils constituent des œuvres au sens de l'article 2 de la *Loi sur le droit d'auteur*[449]. La *Loi sur le droit d'auteur* prévoit en effet que l'organisme public détenant un exemplaire numérique d'une œuvre (qu'il s'agisse d'un logiciel, d'une application, ou d'un fichier) ne pourra pas la communiquer au public par télécommunication[450] sans obtenir l'autorisation du titulaire de ladite œuvre[451]. Or, le fait de donner un accès public à un contenu protégé par droit d'auteur via le nuage « de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement »[452] constitue une telle communication proscrite, sous réserve de certaines exceptions prévues à la *Loi sur le droit d'auteur*[453]. Notons que l'expression « accès public » ne doit pas ici être interprétée comme étant un accès non contrôlé

[447] *Loi sur l'accès*, art. 53. Notons qu'une majorité des textes précités ont une disposition équivalente. Voir par exemple l'article 72.5 de la *Loi sur la protection de la jeunesse.*

[448] Voir, par exemple, l'article 72.5 de la *Loi sur la protection de la jeunesse*; ou l'article 19 de la *Loi sur les services de santé et les services sociaux*.

[449] L.R.C. 1985, c. C-42.

[450] *Loi sur le droit d'auteur*, art. 2.4.

[451] *Loi sur le droit d'auteur*, art. 3.

[452] *Loi sur le droit d'auteur*, art. 2.4 (1.1).

[453] Voir notamment l'article 29.7 de la *Loi sur le droit d'auteur.*

« au public en général »[454]. En effet, « une communication à un groupe restreint de destinataires peut ou non être une communication "au public", selon les circonstances »[455].

Bref, l'entreposage de documents protégés par droit d'auteur dans le nuage ne sera possible que si les accès[456] à ce document sont interdits aux tiers (ce qui inclus le prestataire de services infonuagiques) ou si le titulaire y consent. Par ailleurs, comme – tel que nous le verrons sous peu – les conditions d'utilisation de services infonuagiques prévoient parfois l'octroi d'une licence au prestataire quant aux contenus et applications hébergés dans le nuage, ou encore d'un droit d'accès à ces mêmes informations, ces droits devront également être validés par le titulaire des droits d'auteur.

b) L'obligation de confidentialité

Comme nous l'avons mentionné précédemment, du moment où un document technologique contiendra un renseignement identifié comme étant confidentiel, l'article 25 de la *LCCJTI* prévoit que la personne responsable de l'accès audit document, en l'occurrence le ministère ou l'organisme responsable de sa détention[457], devra « prendre les mesures de sécurité propres à en assurer la confidentialité » [458]. Est-ce dire que cette obligation empêche cette personne responsable de confier la conservation à un tiers soit, pour les fins de la présente étude, un prestataire de services infonuagiques ? La réponse à cette question se veut négative.

En effet, l'article 25 *LCCJTI* est complété par l'article 26 de la même loi, lequel prévoit que l'on peut « confier un document technologique à un prestataire de services pour qu'il en assure la

---

[454] *CCH Canadienne Ltée* c. *Barreau du Haut-Canada*, 2002 CAF 187, par. 251 (décision confirmée en appel sur ce point; voir : *CCH Canadienne Ltée* c. *Barreau du Haut-Canada*, 2004 CSC 13, par. 78).

[455] Marc BARIBEAU, Sylvain GADOURY et Patrick GINGRAS, *Principes généraux de la Loi sur le droit d'auteur*, Québec, Publications du Québec, 2013, p. 17. Par exemple, l'article 2.4 de la LDA prévoit notamment que : « font partie du public les personnes qui occupent les locaux d'un même immeuble d'habitation, tel un appartement ou une chambre d'hôtel, et la communication qui leur est exclusivement destinée est une communication au public ».

[456] Notons que la notion d'« accès » est ici utilisée selon le sens qui lui est accordé par l'article 2.4 de la *Loi sur le droit d'auteur*, et non au sens prévu à la *Loi sur l'accès*.

[457] Voir l'article 1 de la *Loi sur l'accès.*

[458] *LCCJTI*, art. 25.

garde »[459]. Toutefois, lorsque le document en question renferme des renseignements confidentiels, il faudra « informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance »[460]. Notons que cette obligation ne libère pas la personne responsable de l'accès de sa propre obligation d'assurer la confidentialité des données tant en vertu de l'article 25 que des lois sectorielles ou particulières à certains types de données (données fiscales, médicales, etc.). Ainsi, si le prestataire de services infonuagiques omet de mettre en place les mesures de sécurité convenues et que la confidentialité des renseignements personnels d'un citoyen est compromise, l'organisme public ou le ministère demeurera responsable des lacunes sécuritaires.

Bref, si l'obligation de confidentialité des ministères et organismes publics n'empêche pas le recours à l'infonuagique, il demeure qu'un ministère ou un organisme public désirant confier les renseignements personnels de citoyens à un prestataire de services infonuagiques se verra dans l'obligation de mettre en place certaines mesures de sécurité[461] et/ou d'exiger que le prestataire de services infonuagiques procède à la mise en place de telles mesures[462] afin d'empêcher tout tiers (qu'il s'agisse d'un état, d'une entreprise ou d'un particulier) d'avoir accès, soit volontairement, soit par erreur, aux données confidentielles hébergées.

Pour ce faire, plusieurs procédés et technologies peuvent être mis en œuvre dont ceux énumérés à l'article 25 de la *LCCJTI*, à savoir :

- un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite;

[459] *LCCJTI*, art. 26. Notons que cette posibilité est également prevue à l'article 1er de la *Loi sur l'accès*, lequel prévoit que la conservation d'un document détenu par un organisme public peut être confiée à un tiers.

[460] *LCCJTI*, art. 26.

[461] *LCCJTI*, art. 25.

[462] *LCCJTI*, art. 26.

- un contrôle d'accès effectué au moyen d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement[463].

Ces contrôles d'accès peuvent notamment impliquer l'utilisation de mesures de chiffrement des données, de mots de passe, etc., et varieront selon le type de renseignements collectés. En effet, il importe de rappeler que l'article 63.1 de la *Loi sur l'accès* prévoit que les mesures de sécurité à mettre en place doivent être raisonnables selon la sensibilité, la finalité, la quantité et la répartition des renseignements, laissant donc transparaître qu'il s'agit d'une obligation de moyen[464]. Ainsi, certains renseignements plus sensibles (numéro d'assurance sociale[465], renseignements médicaux[466], données fiscales[467], etc.) requerront un niveau de sécurité accru.

Dans de tels cas, les risques associés au recours à un service d'infonuagique publique – aussi faibles soient-ils lorsqu'un cadre contractuel adéquat est mis en place – semblent inconciliables avec le niveau de sensibilité des renseignements. Pour tout autre renseignement, l'évaluation des risques devra être effectuée pour identifier le niveau de sécurité adéquat dans chaque circonstance. Un parallèle peut ici être effectué avec les recommandations du *Code type sur la protection des renseignements personnels*[468] :

---

[463] *LCCJTI*, art. 25. L'article 4.7.3 de l'annexe 1 à la *LPRPDÉ* – lequel n'est pas applicable aux organismes publics québécois – propose quant à lui de mettre ne place : a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux; b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et; c) des mesures techniques, par exemple, l'usage de mots de passe et du chiffrement.

[464] L'obligation de moyen est celle « en vertu de laquelle le débiteur est tenu, non pas d'obtenir un résultat précis, mais uniquement de mettre en œuvre tous les moyens pour y parvenir », H. REID, préc., note 411, p. 425. Sur le fait que l'article 63.1 de la *Loi sur l'accès* impose une obligation de moyen, voir : Martin DUBOIS, « Nouvelles technologies de l'information et des communications et sécurité informationnelle », dans Service de la formation permanente du Barreau du Québec, *Développements récents en droit de l'accès à l'information (2002)*, EYB2002DEV565. Pour une analyse plus complète de l'intensité de l'obligation de sécurité, voir N. W. VERMEYS, préc., note 129, p. 95 et ss.

[465] *Lehman* c. *Pratt & Whitney Canada Corporation*, 2007 QCCS 3888, par. 3.

[466] *Loi concernant le partage de certains renseignements de santé*, RLRQ c. P-9.0001. Notons que cette loi est la seule à souligner expressément qu'un organisme se doit de protéger la confidentialité, la disponibilité et l'intégrité de renseignements spécifiques, en l'occurrence des renseignements médicaux (art. 2 (9°)).

[467] *Loi sur l'administration fiscale*, art. 69.

[468] CAN/CSA-Q830-96. Ce doccument constitue l'Annexe 1 à la *LPRPDÉ*.

> « Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être. »[469]

Une fois qu'il est établi que le transfert de documents contenant des données confidentielles vers les serveurs d'un prestataire de services infonuagiques est possible, il nous faut nous pencher sur les principales craintes associées à une telle migration. D'abord, soulignons l'inquiétude grandissante des organismes publics quant à la situation géographique du prestataire de services infonuagiques ou de ses serveurs. En effet, comme nous le verrons, même lorsque le prestataire de services infonuagiques s'engage contractuellement à assurer la confidentialité des informations dont il a la garde, cet engagement peut parfois être invalidé par des dispositions législatives qui l'obligent à communiquer certaines informations à l'état ou à un tiers (i). Ensuite, le prestataire de services infonuagiques lui-même peut s'attribuer certains droits ou certains pouvoirs relatifs aux données hébergées sur ses serveurs, lesquels droits seront souvent incompatibles avec les obligations des organismes publics (ii).

Mentionnons au passage que, si ces préoccupations sont souvent associées aux cas d'hébergement de données dans le nuage, elles ne se limitent pas à ce modèle de service. En effet, dans le cas où une application située dans le nuage permet l'accès, le traitement ou la consultation de renseignements confidentiels, ces renseignements se retrouveront dans le nuage pour la durée du traitement, voire même plus longtemps selon la politique de conservation des données en place. Ainsi, par exemple, l'utilisation d'une application de type tableur offerte selon un modèle SaaS implique que les données utilisées pour créer un tableau seront accessibles dans le nuage durant la période de préparation dudit tableau, même si celui-ci est sauvegardé sur le poste de travail de l'utilisateur. Il importe donc de bien comprendre que les risques énoncés ci-après sont présents à travers les différents modèles de service dès lors qu'ils transfèrent, même ponctuellement, des renseignements personnels dans le nuage.

---

[469] *LPRPDÉ*, annexe 1, art. 4.3.4.

i) L'obligation de confidentialité lorsque le prestataire de services infonuagiques est situé à l'extérieur du Québec

Selon les débats parlementaires entourant l'adoption de la *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*[470], le contrat visant l'hébergement de renseignements personnels avec un autre organisme public, voire même une entreprise privée, serait associé à une communication de données à cet organisme ou cette entreprise[471]. En effet, « 67.2 parle de ces contrats d'impartition, il parle de la forme dans laquelle on doit les donner et quelles conditions on doit assortir avec ces contrats »[472]. Or, selon cette disposition, « [u]n organisme public peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme ». Cette possibilité s'étendrait également à l'hébergement du « secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle »[473] puisque l'article 41.2 de la même loi prévoit que :

> 41.2. Un organisme public peut communiquer un renseignement visé par une restriction au droit d'accès prévue aux articles 23, 24, 28, 28.1 ou 29 dans les cas suivants:
>
> […]
>
> 6° à toute personne ou tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise confié par l'organisme public à cette personne ou à cet organisme. (notre soulignement)

---

[470] Projet de loi n° 86 : *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, 2006, chapitre 22.

[471] QUÉBEC, ASSEMBLÉE NATIONALE, *Journal des débats de la Commission permanente de la culture*, 2e sess., 37e légis., 30 mai 2006, « Étude détaillée du projet de loi n° 86 – *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives* », p. 1-45.

[472] *Id.*, 12h20 (M. Bédard).

[473] *Loi sur l'accès*, art. 23.

Bref, selon l'interprétation de la *Commission permanente de la culture*, la communication de renseignements confidentiels à un prestataire de services infonuagiques serait autorisée par le biais de l'article 67.2 de la *Loi sur l'accès*. Toutefois, le législateur impose quelques restrictions à une telle communication. Par exemple, si le prestataire de services infonuagiques est une entreprise privée, l'organisme public se devra :

> « [d']indiquer, dans le mandat ou le contrat, les dispositions de la présente loi qui s'appliquent au renseignement communiqué au mandataire ou à l'exécutant du contrat ainsi que les mesures qu'il doit prendre pour en assurer le caractère confidentiel, pour que ce renseignement ne soit utilisé que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne le conserve pas après son expiration. En outre, l'organisme public doit, avant la communication, obtenir un engagement de confidentialité complété par toute personne à qui le renseignement peut être communiqué, à moins que le responsable de la protection des renseignements personnels estime que cela n'est pas nécessaire. Une personne ou un organisme qui exerce un mandat ou qui exécute un contrat de service visé au premier alinéa doit aviser sans délai le responsable de toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué et doit également permettre au responsable d'effectuer toute vérification relative à cette confidentialité. »[474]

Si l'hébergeur est membre d'un ordre professionnel, tel un avocat ou un notaire, ou s'il est lui-même un organisme public (pensons par exemple au *Centre de services partagés du Québec*), de telles précautions ne seront pas nécessaires.

Qu'en est-il, toutefois, lorsque l'hébergeur est une entreprise étrangère ou, encore, une entreprise québécoise dont les serveurs sont situés à l'extérieur du Québec ? Dans un tel cas, l'article 67.2 de la *Loi sur l'accès* doit être lu conjointement avec l'article 70.1 de la même loi, lequel est à l'effet que :

> « Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi.

[474] *Loi sur l'accès*, art. 67.2, al. 2.

> Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte. »[475]

Largement inspirée de l'article 17[476] de la *LPRPSP*[477], cette disposition – entrée en vigueur en 2006 – a fait l'objet de très peu d'analyse et de discussion dans la jurisprudence et la doctrine.

Selon Raymond Doray et François Charette, l'article 70.1 de la Loi implique que, « [s]i les personnes ou les organismes qui recevront les renseignements personnels dans une autre juridiction sont assujettis à une loi sur la protection des renseignements personnels similaire à la loi du Québec, on peut conclure que les renseignements en question recevront une protection équivalente »[478]. Les auteurs poursuivent en précisant que « [l]e respect de l'article 70.1 requerra donc une analyse rigoureuse des lois relatives à la protection des renseignements personnels applicables aux organismes publics ou aux personnes ou organismes privés qui recevront les renseignements dans l'autre juridiction »[479].

---

[475] *Loi sur l'accès*, art. 70.1.

[476] « 17. La personne qui exploite une entreprise au Québec et qui communique à l'extérieur du Québec des renseignements personnels ou qui confie à une personne à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer:

1° que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées sauf dans des cas similaires à ceux prévus par les articles 18 et 23;

2° dans le cas de listes nominatives, que les personnes concernées aient une occasion valable de refuser l'utilisation des renseignements personnels les concernant à des fins de prospection commerciale ou philanthropique et de faire retrancher, le cas échéant, ces renseignements de la liste.

Si la personne qui exploite une entreprise estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions prévues aux paragraphes 1° et 2°, elle doit refuser de communiquer ces renseignements ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte ».

[477] Yves D. DUSSAULT, « Modifications au régime de protection des renseignements personnels », (2006) *Repères* EYB2006DEV1265; R. DORAY et F. CHARETTE, préc., note 366, p. III/70.1-1.

[478] R. DORAY et F. CHARETTE, préc., note 366, p. III/70.1-2.

[479] *Id.*

Ainsi, selon cette interprétation, l'organisme public désirant héberger les renseignements personnels de citoyens québécois sur des serveurs situés ailleurs au Canada pourrait procéder de la sorte puisque la loi applicable aux organismes privés ailleurs au pays (à l'exception de la Colombie-Britannique et de l'Alberta et, en matière de renseignements sur la santé, l'Ontario, le Nouveau-Brunswick et Terre-Neuve-et-Labrador) est la *LPRPDÉ*, laquelle a été jugée « essentiellement similaire » à la *LPRPSP* par le gouverneur en conseil[480].

Ont également été jugées essentiellement similaires à la *LPRPDÉ*, la *Personal Information Protection Act*[481] de la Colombie-Britannique, la *Personal Information Protection Act*[482] de l'Alberta, la *Loi de 2004 sur la protection des renseignements personnels sur la santé*[483] de l'Ontario (seulement en ce qui concerne les renseignements sur la santé), la *Loi sur l'accès et la protection en matière de renseignements personnels sur la santé*[484] du Nouveau-Brunswick (seulement en ce qui concerne les renseignements sur la santé) et le *Personal Health Information Act*[485] de Terre-Neuve-et-Labrador (seulement en ce qui concerne les renseignements sur la santé). Ainsi, par transitivité[486], ces lois seraient également « essentiellement similaires » à la *LPRPSP*. Or, comme les protections accordées par la *LPRPSP* et la *Loi sur l'accès* sont équivalentes[487], nous sommes d'avis que l'hébergement ailleurs au Canada respecterait les critères de l'article 70.1 de la *Loi sur l'accès*.

Évidemment, ce raisonnement s'appui sur la présomption que les tribunaux québécois partageront l'avis du gouverneur général. En effet, si le gouvernement canadien a admis que la

---

[480] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Lois provinciales essentiellement similaires à la loi fédérale », en ligne : < http://www.priv.gc.ca/leg_c/legislation/ss_index_f.asp >.

[481] SBC 2003, c 63.

[482] SA 2003, c P-6.5.

[483] LO 2004, c 3, ann A.

[484] LN-B 2009, c P-7.05.

[485] SNL 2008, c P-7.01.

[486] En mathématique, « se dit d'une relation qui, lorsqu'elle lie un premier terme à un second, et ce second à un troisième, lie de la même façon le premier terme au troisième ». Voir < http://dictionnaire.reverso.net/francais-definition/transitivit%C3%A9 >.

[487] En effet, la lettre de plusieurs des articles des deux textes de loi est identique.

LPRPSP était essentiellement similaire à la *LPRPDE*, cette reconnaissance n'a jamais été confirmée par une quelconque autorité québécoise. La reconnaissance, par les tribunaux québécois, de l'équivalence des protections accordées par la *LPRPDÉ* à celles accordée par la *Loi sur l'accès* n'est donc pas acquise, bien qu'elle puisse être présumée.

La même logique transitive s'appliquerait également aux pays membres de l'Union européenne puisque la *LPRPDÉ* a aussi été jugée comme offrant « un niveau de protection adéquat des données à caractère personnel »[488] pour permettre aux entreprises européennes de partager les renseignements personnels de leurs clients avec leurs filiales et partenaires canadiens. En d'autres mots, la *LPRPDÉ* offrirait une protection équivalente à la *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. Ainsi, si la *Loi sur l'accès* offre des protections équivalentes à la *LPRPSP*, que cette dernière est essentiellement similaire à la *LPRPDÉ* et que celle-ci offre un niveau de protection équivalent à la Directive européenne, l'on peut en déduire que la Directive européenne offre des protections équivalentes à la *Loi sur l'accès*[489] en soulignant toutefois, comme pour la *LPRPDÉ*, que l'équivalence a été prononcée par une autorité étrangère (en l'occurrence la Commission européenne) et non une quelconque autorité québécoise ou canadienne, nous empêchant ainsi d'affirmer sans équivoque qu'un tribunal québécois reconnaitra l'équivalence de ces règles législatives. En adoptant cette même logique, il serait possible de prétendre que toutes les lois jugées comme offrant une protection équivalente à la Directive européenne (représentée en vert sur la figure 7 ci-dessous)[490] pourraient également répondre aux exigences de l'article 70.1 de la *Loi sur l'accès*.

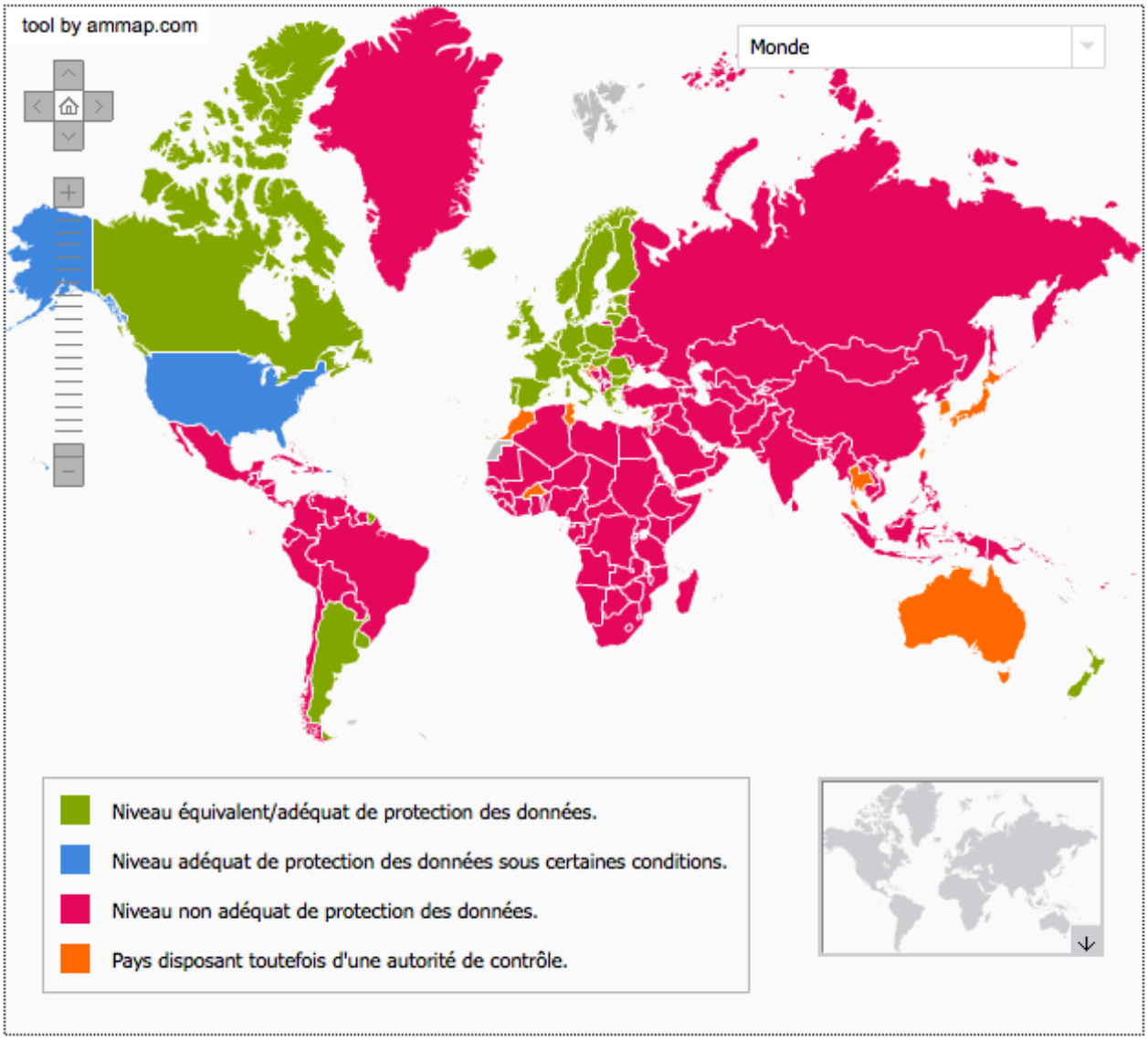
---

[488] 2002/2/CE: Décision de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques [notifiée sous le numéro C(2001) 4539].

[489] Cet avis est notamment partagé par notre collègue Pierre Trudel. Voir Pierre TRUDEL, « Analyse des enjeux et risques juridiques dans le cadre du projet pilote de "coffre-fort électronique" », (2012), à paraître.

[490] Pour une liste de ces lois, voir : CNIL, « Le panorama des législations », (2008), en ligne : < http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/panorama-legislation.pdf >, p. 6.

Figure 7 : Législations nationales en matière de protection des données personnelles[491]



Évidemment, la présence, dans le pays tiers d'un cadre législatif offrant des protections équivalentes à la *Loi sur l'accès* ne libèrera pas l'organisme public québécois des obligations qui lui sont imposées par l'article 67.2 de la même loi (ou par l'article 26 de la *LCCJTI*), c'est-à-dire qu'il devra tout de même mettre en place un cadre contractuel prévoyant les mesures à implémenter pour assurer la confidentialité de l'information hébergée.

[491] Source : CNIL, « Carte des autorités de protection des données dans le monde », en ligne : < http://www.cnil.fr/linstitution/international/les-autorites-de-controle-dans-le-monde/ >.

Qu'en est-il, toutefois, des hébergeurs dont les serveurs sont situés à l'intérieur des frontières de pays dont les lois n'ont pas été considérées comme offrant une protection équivalente à celle assurée par la *Loi sur l'accès* ? Dans certains cas, la mise en place d'un cadre contractuel précis conformément à l'article 67.2 de la *Loi sur l'accès* pourrait être suffisant. Toutefois, lorsque ce cadre contractuel ne pourra résister à une intrusion étatique, notamment lorsque le gouvernement de ce pays se réserve un droit de regard sur toute information hébergée sur son territoire, l'hébergement sera impossible vu la lettre de l'article 70.1 de la *Loi sur l'accès*. Ce serait notamment le cas, à notre avis, pour l'hébergement de données aux États-Unis.

Soulignons d'abord que, contrairement au cadre législatif canadien, les lois états-uniennes relatives à la vie privée n'ont pas été jugées comme offrant « un niveau de protection adéquat des données à caractère personnel » en vertu de la Directive européenne précitée[492]. En effet, l'échange de renseignements personnels entre l'Europe et les États-Unis est régi, comme nous l'avons déjà énoncé, par une série de principes dits de la « sphère de sécurité » (principes Safe Harbour)[493]. Ces principes constituent une série d'exigences auxquelles peuvent se plier les entreprises états-uniennes pour assurer un « niveau de protection adéquat pour le transfert de données de la Communauté vers les États-Unis d'Amérique »[494]. Comme l'explique la Commission européenne :

> « Toute organisation est libre de remplir ou non les conditions relatives à la "sphère de sécurité" et dispose de plusieurs moyens pour s'y conformer. Les organisations qui décident d'adhérer aux principes doivent les respecter pour obtenir et conserver les avantages de la "sphère de sécurité" et doivent annoncer publiquement leur décision »[495].

Les principes de la « sphère de sécurité » relatifs à la protection de la vie privée constituent donc un cadre facultatif et volontaire. Pour bénéficier de ses avantages, une entreprise doit :

---

[492] Pour une analyse du cadre législatif états-unien en matière de protection des renseignements personnels voir : Jean-François DE RICO, « L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements », (2014) 6 *Technologies de l'information en bref* 2, 10.

[493] Voir la Décision n° 2000/520/CE du 26 juillet 2000.

[494] *Id.*

[495] *Id.*

1. souligner, dans sa politique publique en matière de protection de la vie privée, qu'elle adhère aux principes de la "sphère de sécurité" et agit en conformité avec ceux-ci;
2. autocertifier son adhésion aux principes, c'est-à-dire déclarer au *U.S. Department of Commerce* qu'elle est en conformité avec les principes. Cette autocertification doit être effectuée annuellement[496].

Dans la foulée des révélations d'Edward Snowden, la Commission européenne est par ailleurs venue préciser que :

1. Les politiques de protection de la vie privée adoptées par les entreprises autocertifiées doivent comporter des informations sur la mesure dans laquelle la législation des États-Unis permet aux autorités publiques de collecter et de traiter des données transférées au titre de la sphère de sécurité. En particulier, les entreprises devraient être encouragées à indiquer, dans leurs politiques de protection de la vie privée, quand elles dérogent auxdits principes pour répondre à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois.
2. Il importe de ne recourir à la dérogation pour raison de sécurité nationale, prévue par la décision relative à la sphère de sécurité, que dans la mesure où cela est strictement nécessaire et proportionné[497].

À la lumière de ce qui précède, l'on peut se demander si les prestataires de services infonuagiques qui acceptent de s'autocertifier en vertu des principes de la sphère de sécurité pourraient eux aussi, par transitivité, êtres considérés comme offrant protection équivalant à celle prévue à la *Loi sur l'accès*. À notre avis, et malgré ce qu'en disent certains auteurs[498], cette équivalence serait difficile à démontrer. D'abord, notons que la Commission européenne, tout en

[496] « Une entreprise américaine souhaitant adhérer aux principes de la sphère de sécurité doit: a) stipuler, dans la politique de protection de la vie privée qu'elle publie, son adhésion auxdits principes, et s'y conformer effectivement, et b) s'autocertifier, c'est-à-dire déclarer au ministère du commerce qu'elle est en conformité avec lesdits principes. L'autocertification doit être annuellement renouvelée ». Voir : COMMISSION EUROPÉENNE, « Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis — Foire aux questions », MEMO/13/1059, 27 novembre 2013.

[497] *Id.*

[498] J.-F. De RICO, préc., note 492, 9.

admettant que le respect des principes de sphère de sécurité permet de bénéficier de la présomption de « niveau de protection adéquat »[499] vient tout de même préciser que les principes :

> « sont exclusivement destinés aux organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne et doivent permettre à ces organisations de remplir les conditions relatives à la "sphère de sécurité" de façon à bénéficier de la présomption de "niveau de protection adéquat" que prévoit celle-ci. Comme les principes n'ont été conçus que pour servir cet objectif spécifique, leur adoption à d'autres fins peut s'avérer inadéquate. Les principes ne peuvent pas se substituer aux dispositions nationales de mise en œuvre de la directive qui sont applicables au traitement des données à caractère personnel dans les États membres. »[500]

Ensuite, et surtout, comme les principes ne constituent pas un texte législatif, ils n'offrent en fait aucune protection supérieure à une entente contractuelle. Or, s'il est vrai que : « [s]i, dans cette autre juridiction, il n'existe pas de loi qui assure une protection équivalente des renseignements personnels ou si la loi applicable dans cette autre juridiction est moins sévère en termes de protection des renseignements personnels que la loi québécoise, il sera possible de recourir à des ententes contractuelles »[501], lorsque la législation en vigueur dans le pays où l'information est vouée à être hébergée rend ce cadre contractuel inefficace, le second alinéa de l'article 70.1 de la *Loi sur l'accès* doit trouver application. Or, à notre avis, cet alinéa proscrit l'hébergement d'informations confidentielles aux États-Unis puisqu'elle serait alors soumise à la *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, mieux connue sous l'acronyme *USA PATRIOT Act*, à laquelle nous avons déjà fait référence dans la première partie de la présente étude.

Comme le souligne Cynthia Chassigneux, cette loi « permet aux autorités américaines, par ordonnance d'un tribunal, d'obtenir la communication de renseignements identifiant une personne physique n'étant pas de citoyenneté américaine dès lors que ces informations sont conservées sur

---

[499] Décision n° 2000/520/CE.

[500] *Id.*

[501] Voir R. DORAY et F. CHARETTE, préc., note 366, p. III/70.1-2.

le territoire américain »[502]. L'auteure poursuit en précisant que « [c]ette communication se fait à l'insu non seulement de la personne concernée, mais aussi de l'entité juridique qui a imparti ou confié la sous-traitance des renseignements personnels qu'elle a collecté à un tiers situé aux États-Unis »[503]. Nous sommes donc d'avis que ce droit accordé aux autorités américaines est incompatible avec la lettre de l'article 70.1 de la *Loi sur l'accès*. D'ailleurs, tel que le soulève Yves D. Dussault, l'article 70.1 de la *Loi sur l'accès* a justement été adopté « dans la foulée notamment de certaines préoccupations soulevées par l'adoption aux États-Unis de la *USA Patriot Act* qui facilite la transmission de renseignements personnels au FBI »[504]. La lecture du journal des débats relatifs au projet de loi 86 (*Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*), lequel donna naissance à l'article 70.1 de la *Loi sur l'accès*, démontre en effet une préoccupation marquée, de la part des membres de l'Assemblée nationale, quant à l'hébergement de renseignements personnels en sol américain[505].

Notons par ailleurs que cette préoccupation ne se limite pas aux entreprises dont les serveurs sont situés en sol américain. Elle s'étend également aux entreprises américaines dont les serveurs pourraient être situés au Québec. En effet, il est utile de préciser que l'article 70.1 de la *Loi sur l'accès* ne vise pas uniquement « les renseignements communiqués à l'extérieur du Québec », il s'applique également aux « personnes ou organismes situés à l'extérieur du Québec ». En effet, tel que l'a démontré l'affaire *eBay Canada Ltd.* c. *M.R.N.*[506], les lois d'un état peuvent s'étendre aux serveurs d'une entreprise situés à l'extérieur de cet état. Comme le souligne la Cour d'appel fédérale dans cette affaire, « les renseignements électroniques stockés sur des serveurs situés à

[502] C. CHASSIGNEUX, préc., note 228, aux pages 64 et 65.

[503] *Id.*, à la page 65.

[504] Y. D. DUSSAULT, préc., note 477.

[505] Voir QUÉBEC, ASSEMBLÉE NATIONALE, préc., note 471, p. 1-45; et QUÉBEC, ASSEMBLÉE NATIONALE, *Journal des débats de la Commission permanente de la culture*, 2e sess., 37e légis., 31 mai 2006, « Étude détaillée du projet de loi n° 86 – Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives », p. 11-32.

[506] 2008 CAF 348.

l'étranger peuvent en droit être dits situés au Canada »[507]. Or, comme nous l'avons déjà abordé, cette vision est partagée par les autorités états-uniennes :

> « The U.S. government has ample possibilities to request data from foreign (in this case Dutch) users of the cloud. The most striking example in this regard is the specific provision (50 USC § 1881a) introduced in 2008 for the acquisition of data of non-U.S. persons outside the United States, given the far-reaching powers it grants to retrieve information on a large scale, including access to complete data sets. U.S. authorities also have powers to request information from cloud providers in the context of criminal investigations. Jurisdiction under U.S. law is a necessary precondition, which is effectuated when cloud providers are based in the United States or if they conduct continuous and systematic business in the United States. It is a misconception that U.S. jurisdiction applies only if the data are physically located on U.S. territory. »[508]

D'ailleurs, il a été appris, à la lumière de documents diffusés par Edward Snowden, que Microsoft aurait collaboré avec le NSA pour permettre l'accès à ses serveurs d'infonuagique :

> « Microsoft's cloud storage service SkyDrive is also easy to access, thanks to Redmond's work with the NSA. The agency reported on April 8, 2013 that Microsoft has built PRISM access into Skydrive in such a way as to remove the need for NSA analysts to get special authorization for searches in Microsoft's cloud. »[509]

Or, les serveurs de Microsoft, s'ils sont majoritairement situés aux États-Unis, se retrouvent également en Amérique du Sud, en Europe, en Asie et en Australie :

---

[507] *Id.*, par. 52.

[508] J. VAN HOBOKEN, A. ANRBAK et N. VAN EIJK, préc., note 195.

[509] Iain THOMSON, « Snowden leak: Microsoft added Outlook.com backdoor for Feds », (2013) *The Register*, en ligne : < http://www.theregister.co.uk/2013/07/11/snowden_leak_shows_microsoft_added_outlookencryption_backdoor_for_feds/ >.

Figure 8 : Situation géographique des serveurs de Microsoft[510]

Cette dernière observation nous permet de revenir sur une autre problématique de l'hébergement de données « dans le nuage » d'une entreprise. En effet, puisque, comme nous venons de le voir, les serveurs d'un hébergeur sont souvent situés dans plus d'un état, il devient difficile d'identifier où se trouvent nos données. Qui plus est, les hébergeurs se réservent souvent le droit de transférer les données d'abonnés d'un serveur à l'autre et, donc, d'un continent à l'autre. Par exemple, la politique de vie privée de Google Cloud prévoit que : « Google processes personal information on our servers in many countries around the world. We may process your personal information

[510] Source : Bart VANDE GHINSTE, « Microsoft Cloud Continuum », (2010), en ligne : < http://download.microsoft.com/download/7/3/C/73CACA9C-009D-46DC-88A2-5D92E1460A64/Hansver_I3_ISV_Cloud%20public.pptx >.

on a server located outside the country where you live »[511]. L'article 70.1 de la *Loi sur l'accès* impose donc l'analyse du cadre législatif en place non seulement dans le pays du gestionnaire du nuage, mais également dans chaque pays où sont situés ses serveurs. Comme cette vérification est souvent impossible (en effet, rares sont les prestataires de services infonuagiques qui communiquent l'emplacement exact de tous leurs serveurs), l'article 70.1 rendrait le recours à un nuage public difficilement justifiable.

Évidemment, cette impossibilité de recourir au nuage ne serait valide que dans le cas de renseignements **personnels** dont la confidentialité se doit d'être assurée en vertu de la *Loi sur l'accès*. Ainsi, une telle interdiction ne s'étendrait pas aux renseignements visés par l'article 53 de la *Loi sur l'accès* ou aux données publiques.

L'analyse des articles 67.2 et 70.1 de la *Loi sur l'accès* que nous venons d'effectuer, ou plutôt l'interprétation qui en découle, si elle est conforme à ce qui découle des débats parlementaires entourant l'adoption de ces dispositions et à la position mise de l'avant par certains auteurs[512], n'est toutefois pas exempte de critiques. En effet, bien que l'intention du législateur semble – si l'on se fie au journal des débats[513] – être à l'effet qu'un contrat d'hébergement soit soumis à l'article 67.2 de la *Loi sur l'accès*, nous sommes d'avis que la lettre de cette disposition est difficilement conciliable avec une telle affirmation. En effet, comme nous l'avons indiqué ci-dessus, les articles 67.2 et 70.1 de la *Loi sur l'accès* visent principalement la « communication » de renseignements personnels ou autrement confidentiels. Or, la notion de « communication » n'est pas définie dans la *Loi sur l'accès*, ni par ailleurs dans les autres textes connexes[514]. Selon l'interprétation précitée, la notion de communication serait synonymique de « transmission », soit l'« [e]nvoi de données ou d'un signal, d'un point à un autre, en utilisant un ensemble de moyens

[511] GOOGLE, « Privacy Policy », en ligne : < http://www.google.com/intl/en/policies/privacy/ > (dernières modifications : 24 juin, 2013).

[512] Voir R. DORAY et F. CHARETTE, préc., note 366, p. III/70.1-2.

[513] Préc., note 471.

[514] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Thémis, 2010, p. 96.

spécialisés telle une ligne de communication »[515], toutefois, selon l'Office de la langue française, cette définition serait incomplète puisque, pour qu'il y ait communication, la transmission doit être accompagnée du décodage de l'information transmise[516]. D'ailleurs, la *Loi sur l'accès* semble reconnaître l'idée que la communication implique une prise de connaissance de l'information transmise puisqu'elle associe, à maintes reprises, la communication à une divulgation (ou tout au moins un risque de divulgation) de renseignements[517].

Or, les organismes publics lorsqu'ils confient des documents technologiques à un prestataire de services infonuagiques, ne visent pas à lui divulguer le contenu desdits document ou encore à lui permettre d'en prendre connaissance, ils visent seulement à accorder à ce dernier la garde[518] ou la conservation de documents[519]. Or : « La conservation d'un document est aussi une opération distincte de la communication et ce n'est pas parce qu'une entité conserve un document, qu'elle a le droit d'y accéder ou de le communiquer »[520] (nos soulignements).

Ainsi, le contrat de prestation de services infonuagiques (particulièrement lorsque le modèle retenu implique l'hébergement de données dans le nuage) ne viserait pas la communication, mais uniquement la conservation de documents[521]. Selon cette analyse textuelle, les contrats de prestation de service d'infonuagique ne seraient donc pas soumis à l'application de l'article 67.2

---

[515] OLF, préc., note 3.

[516] *Id.*

[517] Voir notamment les articles 19, 20, 21, 22, 24, 27, 28, 28.1, 29, 29.1, 30.1, 32, 41, 88 de la *Loi sur l'accès*. Voir également V. GAUTRAIS et P. TRUDEL, préc., note 514, p. 227. Les auteurs sont en effet d'avis que la communication « implique un droit de prendre connaissance de la teneur du document ou du renseignement ». Cette position est par ailleurs développée aux pages 95 et ss. du même ouvrage. Cette prise de position nous semble conforme à l'article 59 de la *Loi sur l'accès*, lequel prévoit les cas dans lesquels un organisme peut communiquer un renseignement personnel.

[518] *LCCJTI*, art. 26.

[519] Notons que ces deux notions sont synonymiques. Voir V. GAUTRAIS et P. TRUDEL, préc., note 514, p. 128.

[520] *Id.*, p. 133. Cette position est d'ailleurs conforme aux articles 22 et 27 de la *LCCJTI*, lesquels prévoient expressément que la notion de conservation n'est liée à aucune obligation de surveillance.

[521] Notons que ces deux notions sont clairement traitées de façon distincte dans la *Loi sur l'accès*. À cet effet, voir notamment l'article 89 de la Loi, lequel prévoit que : « [t]oute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié » (notre soulignement).

de la *Loi sur l'accès*. Si cette position ne semble pas conforme aux propos reproduits dans le journal des débats[522], rappelons que, « [l]orsque le texte de la loi est clair et sans ambiguïté, aucune autre démarche n'est nécessaire pour établir l'intention du législateur »[523].

Ce raisonnement viendrait également possiblement soustraire les contrats de prestation de services infonuagiques à l'application de l'article 70.1 de la *Loi sur l'accès*. En effet, rappelons que cette disposition vise :

- la communication à l'extérieur du Québec des renseignements personnels;
- le fait de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir des renseignements personnels;
- le fait de confier à une personne ou à un organisme à l'extérieur du Québec la tâche d'utiliser des renseignements personnels;
- le fait de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de communiquer des renseignements personnels.

Nous venons de le voir, l'organisme public qui héberge des renseignements personnels ou autrement confidentiels dans le nuage ne communique pas ceux-ci au prestataire de service d'infonuagique et, il va de soi, ne confie pas non plus à ce dernier la tâche d'utiliser ou de communiquer ces mêmes renseignements. Ainsi, pour que l'hébergement de données dans le nuage soit soumis à l'article 70.1 de la *Loi sur l'accès*, il est nécessaire de démontrer que la **détention** de renseignements personnels a été confiée au prestataire. Or, selon l'article 1er de la *Loi sur l'accès*, ladite loi « s'applique aux documents détenus par un organisme public dans l'exercice de ses fonctions, que leur conservation soit assurée par l'organisme public ou par un tiers » (nos soulignements). Ainsi, en invoquant la méthode systématique et logique d'interprétation des lois[524], il serait possible de prétendre que cette disposition implique que la **détention** d'un document est assurée par l'organisme public même lorsque la **conservation** de

[522] Préc., note 471.

[523] *R.* c. *Multiform Manufacturing Co.*, [1990] 2 R.C.S. 624, 630 (j. en chef Lamer). Propos tels que rapportés dans P.-A. CÔTÉ, préc., note 403, p. 290.

[524] Voir P.-A. CÔTÉ, préc., note 403, p. 351 et ss.

celui-ci est confiée à un tiers[525]. Notons toutefois que, pour que cette analyse soit acceptée, il faudrait prétendre que la détention prévue à l'article 70.1 n'est qu'une détention juridique. En effet, l'interprétation faite tant par la doctrine[526] que par les tribunaux[527] de l'article 1er de la *Loi sur l'accès* est à l'effet que, même si l'organisme public conserve la détention **juridique** des renseignements, il peut en céder la détention **physique** :

> « L'article 1 de la *Loi d'accès* prévoit que la Loi s'applique à tous les documents, que la conservation de ces derniers soit assurée par l'organisme public ou par un tiers […]. La Loi ne fait aucune distinction entre la conservation ou détention juridique et la détention physique. Au contraire, l'article 1 prévoit que dès qu'un organisme est dans l'exécution de ses fonctions, il peut y avoir une demande d'accès à des documents relatifs à une de ces fonctions, que ces documents soient détenus par l'organisme ou par un tiers. »[528]

Bref, une analyse téléologique[529] de l'article 70.1 permettrait possiblement de désamorcer les arguments précités. Toutefois, ces arguments ne visaient pas autant à trouver une façon de permettre l'hébergement de documents technologiques contenant des renseignements personnels à l'extérieur du Canada, mais plutôt à souligner les lacunes de l'article 70.1 de la *Loi sur l'accès* et des risques juridiques générés par la terminologie utilisée (détenir *versus* conserver, communiquer *versus* transmettre).

En effet, même si l'on acceptait l'analyse textuelle de la *Loi sur l'accès* que nous venons d'effectuer, nous sommes d'avis que l'hébergement, sur les serveurs d'un prestataire de services infonuagiques étranger des renseignements personnels détenus par un organisme public québécois, pourrait tout de même contrevenir aux obligations juridiques de cet organisme. En effet, rappelons que, au-delà des obligations spécifiques de confidentialité imposées aux organismes publics par la *Loi sur l'accès*, les organismes publics sont également soumis à

---

[525] Voir V. GAUTRAIS et P. TRUDEL, préc., note 514, p. 228.

[526] R. DORAY et F. CHARETTE, préc., note 366, p. I/1-4 et ss.

[527] Voir notamment *Gyulai* c. *Montréal (Ville de)*, 2009 QCCQ 1809 (confirmée par la Cour supérieure dans *Montréal (Ville de)* c. *Cour du Québec*, 2009 QCCS 2895, puis infirmée par la Cour d'appel dans *Montréal (Ville de)* c. *Gyulai*, 2011 QCCA 238) pour une analyse de l'interprétation de la notion de détention à l'article 1er de la *Loi sur l'accès*.

[528] *Office du crédit agricole du Québec* c. *Boucher*, préc., note 366, 254.

[529] Voir P.-A. CÔTÉ, préc., note 403, p. 441 et ss.

l'obligation générale de « prendre les mesures de sécurité propres à assurer la confidentialité » des renseignements confidentiels qu'ils détiennent, « notamment par un contrôle d'accès effectué au moyen […] d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement »[530]. Or, comme le gouvernement américain est « une personne non autorisée » en vertu du droit québécois, l'hébergement aux États-Unis demeurerait problématique.

Qui plus est, s'il est facile, à la lumière de l'affaire Snowden, de pointer du doigt Washington et de souligner la portée abusive du *USA PATRIOT Act*, il importe de rappeler que le législateur états-unien n'est pas seul à s'être accordé un pouvoir de surveillance accru au lendemain du 11 septembre 2001. En effet, la *Loi antiterroriste canadienne*[531] renferme également certaines dispositions qui « renforcent les pouvoirs d'investigation des autorités publiques en vue d'assurer la sécurité nationale et, corrélativement, internationale »[532], tout comme la France[533], l'Angleterre[534], etc.[535].

Il est donc légitime de se demander si le fait qu'un renseignement confidentiel hébergé à l'étranger puisse être consulté par les autorités de ce pays est suffisant pour rendre l'hébergement de données dans ledit pays impossible en vertu des obligations qui incombent aux organismes publics québécois. À cette question, il est intéressant de mentionner la réponse de la commissaire adjointe à la protection de la vie privée du Canada. Selon cette dernière :

> « même si l'on devait examiner la question de la "protection comparable" sous l'angle des lois antiterroristes des États-Unis par rapport à celles du Canada, il est clair, selon la commissaire ajointe, qu'il existe un risque juridique comparable que des organismes gouvernementaux aient accès aux renseignements personnels de Canadiennes et de Canadiens détenus par une

[530] *LCCJTI*, art. 25.

[531] LC 2001, c 41.

[532] C. CHASSIGNEUX, préc., note 228, à la page 64. Voir également J.-F. De RICO, préc., note 492, 12.

[533] *Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*.

[534] *Anti-terrorism, Crime and Security Act 2001*, 2001 c. 24.

[535] Pour une analyse du pouvoir de surveillance accordé à l'état dans ces différents pays, voir : Jennifer STODDART, « Pouvoirs de surveillance, de perquisition ou de saisie élargis par des lois récentes au Canada, au Royaume-Uni, en France et aux États-Unis », (2009), en ligne : < http://www.priv.gc.ca/parl/2009/parl_bg_090507_f.pdf >.

> organisation et par son fournisseur de services – qu'il soit canadien ou américain – par le biais des lois américaines ou des lois canadiennes. »[536]

Ainsi, selon cette logique (laquelle, il importe de le souligner, ne lie pas les organismes publics québécois[537]), puisque le risque juridique dans un pays tiers serait le même qu'au Canada – où le gouvernement canadien possède un pouvoir de surveillance en vertu de la *Loi antiterroriste* – l'obligation de confidentialité serait respectée si un cadre contractuel est mis en place. Notons au passage que certains auteurs proposent l'application de cette même logique aux entreprises privées québécoises soumises à la *LPRPSP*[538]. Bref, l'hébergement à l'étranger, même aux États-Unis, serait donc envisageable, bien que l'argument demeure plus convaincant lorsque le pays hôte possède un corpus législatif offrant une protection équivalente à la *Loi sur l'accès*.

Pourtant, s'il est vrai que le gouvernement canadien détient un certain pouvoir de surveillance quant aux informations hébergées sur des serveurs situés au Canada, il possède, tel que nous l'avons vu, le même pouvoir de surveillance pour les informations situées sur des serveurs accessibles au Canada. C'est donc dire que, en hébergeant des données à l'étranger, l'on soumet celles-ci à la fois au pouvoir de surveillance du Canada **et** du gouvernement étranger, ce qui peut s'avérer inacceptable pour un citoyen québécois qui, par exemple, possède une double nationalité ou qui a un casier judiciaire dans le pays où sont situés les serveurs. Cette problématique ne s'étendrait toutefois pas aux autres provinces canadiennes puisque seul le gouvernement canadien (à l'opposé des gouvernements provinciaux) possède un tel pouvoir de surveillance[539].

La position adoptée par le Commissariat à la protection de la vie privée du Canada se base toutefois sur une logique de libre concurrence qui, si elle peut s'appliquer aux entreprises privées, nous semble difficilement conciliable avec la mission d'une administration gouvernementale[540] :

---

[536] CPVPC, préc., note 93.

[537] *LPRPDÉ*, art. 4.

[538] Voir notamment Karl DELWAIDE, « Quebec Privacy Law Poses Difficulties for Outsourcing of Personal Information », (2007) 27 *Lawyers Wkly.* 14.

[539] *Loi constitutionnelle de 1867*, 30 & 31 Victoria, c 3, art. 91.

[540] CPVPC, préc., note 176.

> « Les organisations doivent aviser leurs consommateurs de façon claire et compréhensible que leurs renseignements personnels pourraient être traités dans un pays étranger, et que les organismes d'application de la loi et de sécurité nationale de ce pays pourraient y accéder. Idéalement, cela devrait être fait au moment de la collecte des renseignements. Une fois que des consommateurs avertis décident de faire affaire avec une entreprise, ils ne peuvent s'opposer à ce que leurs renseignements personnels soient transférés. »[541]

En autres mots, le fait de soumettre les données confidentielles concernant un citoyen canadien à une double surveillance étatique (celle du Canada et celle de l'état où sont hébergées les données) n'est pas problématique tant que la personne visée par les renseignements hébergés peut opter de faire affaire avec une autre entreprise dont les données sont uniquement hébergées au Canada. Or, un citoyen québécois ne possède pas un tel choix vis-à-vis du gouvernement du Québec. Un tel citoyen pourrait donc se retrouver sans la possibilité de s'opposer à l'hébergement de ses données à l'étranger, bien qu'un tel hébergement puisse lui causer préjudice. Bref, nous sommes d'avis qu'il serait plus sage de ne faire affaire qu'avec des prestataires de services infonuagiques canadiens dont les serveurs sont tous situés en sol canadien et donc uniquement soumis au pouvoir de surveillance du gouvernement canadien[542].

Une telle proposition, si elle nous semble la seule conforme à la lettre des textes de loi applicables, demeure toutefois difficile à soutenir d'un point de vue pragmatique. En effet, le principe même de l'infonuagique implique la multiplication des serveurs et l'internationalisation du marché. Ainsi, le nombre de prestataires canadiens dont tous les serveurs sont situés au Canada demeure restreint[543]. De plus, ne permettre l'hébergement qu'à l'intérieur du Canada nous semble mal cadrer avec les obligations des organismes publics telles qu'elles découlent

---

[541] *Id.*

[542] Notons que cette recommandation est conforme à ce qui se produit ailleurs au pays. En effet, l'article 30.1 de la *Freedom of Information and Protection of Privacy Act* de Colombie-Britannique impose l'hébergement des données en sol canadien sauf avec l'accord de la personne concernée ou lorsque l'information est publique. Voir OIPCBC, préc., note 215.

[543] Le nombre exact demeure difficile à cerner puisqu'une majorité de prestataires de services ne précisent pas le lieu géographique de leurs serveurs.

d'accords commerciaux signés par le gouvernement du Québec tant au niveau interprovincial[544] qu'international[545]. Par exemple, l'accord sur le commerce intérieur (« ACI »)[546] « vise à établir un cadre qui assurera à tous les prestataires canadiens un accès égal aux marchés publics, de manière à réduire les coûts d'achat et à favoriser l'établissement d'une économie vigoureuse, dans un contexte de transparence et d'efficience ». Ainsi, refuser l'accès aux marchés publics québécois à un prestataire ontarien dont les serveurs sont situés en sol américain pourrait entraîner quelques complications. Au même titre, en vertu de l'Accord intergouvernemental sur les marchés publics entre le gouvernement du Québec et le gouvernement de l'État de New York (AQNY), un organisme québécois serait théoriquement dans l'obligation d'opter pour les services d'un hébergeur new-yorkais si ce dernier remportait un appel d'offre à cet égard[547]. Ceci étant, il importe de préciser qu'un organisme soumis à l'article 63.1 de la *Loi sur l'accès*, lequel, rappelons-le, impose une obligation générale de « prendre les mesures de sécurité propres à assurer la protection des renseignements personnels […] conservés », peut très bien prévoir, dans le cadre d'un appel d'offres pour des services infonuagiques, que l'hébergement des données en sol canadien comporte un avantage comparatif. En effet, l'article 20 de la *Loi sur les contrats des organismes publics*[548] prévoit expressément que « [l]es documents d'appel d'offres doivent prévoir, entre autres […] des dispositions permettant à l'organisme public de s'assurer en tout

[544] Accord de commerce et de coopération entre le Québec et l'Ontario (ACCQO); et Accord de libéralisation des marchés publics du Québec et du Nouveau-Brunswick (AQNB 2008).

[545] Accord intergouvernemental sur les marchés publics entre le gouvernement du Québec et le gouvernement de l'État de New York (AQNY); Accord entre le gouvernement du Canada et le gouvernement des États-Unis d'Amérique en matière de marchés publics (2010); Accord sur les marchés publics (AMP) de l'Organisation mondiale du commerce.

[546] Pour la liste de ces organismes, voir : « Assujettissement aux accords de libéralisation des marchés publics : ministères et organismes du gouvernement ou de l'assemblée nationale », en ligne : < http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/accords/tab_synthese_assujettissement_accords.pdf >.

[547] Il va de soi, évidemment, que l'organisme pourra choisir de ne pas adjuger le contrat (en supposant qu'il se soit réservé cette option). Toutefois, si la volonté est celle de migrer vers l'infonuagique, cette porte de sortie demeure peu utile. Notons par ailleurs que les accords précités ne trouveront application que si le montant du contrat projeté atteint un certain seuil. Voir : « Accords de libéralisation des marchés publics : seuils d'application », en ligne : < http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/accords/tab_synthese_seuils_accords.pdf > et « Synthèse des accords de libéralisation des marchés publics : ministères et organismes du gouvernement », en ligne : < http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/accords/tab_synthese_internet_mo.pdf >.

[548] RLRQ c C-65.1.

temps du respect des règles qui lui sont applicables, notamment en matière d'accès aux documents des organismes publics et de protection des renseignements personnels ». Or, l'ACI, pour reprendre cet exemple, « n'a pas pour effet d'obliger une entité à violer les obligations en matière de confidentialité qui lui sont imposées par la loi »[549]. Toutefois, puisque la portée exacte des articles 67.2 et 70.1 demeure sujette à un certain débat[550], il serait envisageable, pour une entreprise située à l'extérieur du Québec, de prétendre qu'une clause imposant l'hébergement de données au Canada ne respecte pas les accords précités.

Le fait de procéder au chiffrement des données avant de les déposer dans le nuage pourrait être une solution à envisager pour éviter cette problématique tout en répondant aux exigences de la *LCCJTI*. En effet, le chiffrement viendrait respecter l'esprit de la *LCCJTI* et de la *Loi sur l'accès* telle que nous l'avons interprétée en rendant la consultation théoriquement impossible tant pour le prestataire de services infonuagiques que pour un gouvernement étranger quelconque[551]. Ainsi, même si le prestataire détiendrait tout de même les documents, cette détention ne lui permettrait ni de les utiliser, ni de les communiquer, ce qui viendrait répondre aux craintes exprimées lors des débats parlementaires entourant l'adoption du projet de loi 86 même si, encore une fois, la lettre de la loi ne serait, à notre avis, pas respectée.

---

[549] ACI, art. 510.

[550] Voir par exemple J.-F. De RICO, préc., note 492, 7. Contrairement aux soussignés, l'auteur est d'avis que « le libellé des articles 17 et 70.1 qui a été retenu ne permet pas, selon nous, d'attribuer au législateur l'intention d'interdire le recours à des fournisseurs américains ou à des fournisseurs utilisant des installations ou ayant un établissement aux États-Unis ». L'auteur appui son raisonnement sur une interprétation large de l'article 59 (3) de la *Loi sur l'accès*, lequel est à l'effet qu'un organisme peut communiquer un renseignement personnel « à un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est nécessaire aux fins d'une poursuite pour infraction à une loi applicable au Québec » (voir la page 14 de l'article). Pour notre part, nous ne pouvons accepter que cette disposition permet de conclure que « les documents confiés à un prestataire de services en mode infonuagique soumis à la juridiction américaine bénéficieront néanmoins d'une protection équivalente à celle prévue par les lois québécoises qui prévoient également des exceptions à l'interdiction de communication sans consentement en faveur d'un organisme chargé de prévenir, détecter ou réprimer les crimes, lesquels disposent de pouvoir et de mécanismes qui, sous réserve des National Security Letters émises par le FBI, sont assimilables aux prérogatives des autorités américaines » (page 14 de l'article).

[551] Voir David CANELLOS, « Adopting the Cloud While Adhering to Domestic & Foreign Government Regulations », (2013), en ligne : < http://safegov.org/2013/10/2/adopting-the-cloud-while-adhering-to-domestic-foreign-government-regulations >.

Notons toutefois que, nonobstant les risques associés à la disponibilité de l'information énoncés dans la section précédente de la présente étude, si une telle avenue était choisie, l'organisme public se devrait d'utiliser un service de chiffrement distinct de celui offert par le prestataire du service d'infonuagique retenu, sans quoi certains risques pourraient persister, notamment si le prestataire permet à un tiers de prendre copie des renseignements **avant** de procéder au chiffrement des données[552].

ii) L'obligation de confidentialité lorsque le prestataire de services infonuagiques se réserve des droits relatifs aux données hébergées sur ses serveurs

Jusqu'à présent, notre analyse de la portée de l'obligation de confidentialité en ce qui concerne l'infonuagique s'est concentrée sur la possibilité, pour un tiers (qu'il s'agisse d'une autorité étrangère ou d'un bidouilleur[553]), d'avoir accès aux renseignements personnels ou autrement confidentiels détenus par un organisme public québécois. Toutefois, il ne faudrait pas omettre que la confidentialité d'un renseignement pourrait être compromise par le prestataire de services infonuagiques lui-même.

En effet, il est utile de souligner que bon nombre de prestataires de services infonuagiques se réservent un droit de consultation ou d'utilisation des renseignements contenus dans le nuage. Il peut effectivement être surprenant d'apprendre que les conditions d'utilisation de certains services infonuagiques contiennent des clauses contractuelles prévoyant des droits d'accès et d'utilisation quant aux informations hébergées. Par exemple, les conditions d'utilisation du service d'infonuagique Skydrive de Microsoft prévoit que :

> « Toutefois, en mettant en ligne, téléchargeant vers un serveur, saisissant, fournissant ou soumettant votre Contenu (« Mettre en ligne » ou « Mise en ligne »), vous autorisez Microsoft, ses sociétés affiliées et les titulaires de sous-licences concernés à utiliser votre Contenu dans le cadre de leurs activités sur Internet (y compris, notamment, tous les Services Microsoft), et notamment à

[552] « For Prism collection against Hotmail, Live, and Outlook.com emails will be unaffected because Prism collects this data prior to encryption ». Voir I. THOMSON, préc., note 509.

[553] « Personne passionnée d'informatique qui, par jeu, curiosité, défi personnel ou par souci de notoriété, sonde, au hasard plutôt qu'à l'aide de manuels techniques, les possibilités matérielles et logicielles des systèmes informatiques afin de pouvoir éventuellement s'y immiscer ». OLF, préc., note 3. L'expression « bidouilleur » vise donc à la fois le « mordu de l'informatique » n'ayant aucune intention malicieuse et le pirate informatique.

> copier, distribuer, transmettre, afficher publiquement, représenter publiquement, reproduire, modifier, traduire et reformater votre Contenu, à publier votre nom en relation avec votre Contenu, et à sous-concéder ces droits à tout fournisseur des Services. »[554]

Évidemment, de telles clauses sont nécessairement incompatibles avec l'obligation de confidentialité des organismes publics et ne pourraient être acceptées par ceux-ci.

Par ailleurs, bien que cette problématique soit particulièrement évidente lorsque le nuage est utilisé principalement pour l'hébergement de données confidentielles, elle est tout aussi présente pour les différents types de modèles de service énumérés et définis dans la première partie de la présente étude. D'ailleurs, c'est dans le cadre des logiciels sous forme de service qu'elle s'avère être la plus pernicieuse puisque, tel que soulevé précédemment, les outils de collaboration en ligne et autres logiciels sous forme de service tels Google Apps constituent le modèle de service le plus répandu tant à l'intérieur qu'à l'extérieur des administrations gouvernementales[555] et, donc, les principales sources de risques. Qui plus est, comme le souligne un rapport produit par le collectif SafeGov.org, ces outils ne sont pas toujours adaptés aux exigences des organismes publics, mais souvent adoptés parce qu'ils sont « gratuits »[556] : « The most widely used cloud services today are typically free or very inexpensive offerings designed as vehicles for online behavioural advertising aimed at individual consumers »[557]. De cette réalité découlent des risques d'atteintes aux renseignements personnels et autrement confidentiels tant des utilisateurs du service d'infonuagique que de tiers.

- Les risques liés à l'utilisation des logiciels sous forme de service pour les utilisateurs

Pour les utilisateurs d'un service d'infonuagique, les risques sont principalement liés à l'absence de contrôle exercé par ceux-ci sur le service en soi. En effet, pour une majorité de services

[554] MICROSOFT, « Informations sur les conditions d'utilisation », (2012), en ligne : < http://www.microsoft.com/france/core/copyright.aspx >.

[555] Voir la page 33 de la présente étude.

[556] Nous référons ici à une gratuité au sens financier du terme. Nous ne prétendons aucunement que le service n'impose aucun coût pour les utilisateurs.

[557] « Protecting Vulnerable Data Subjects : Findings from a Survey of EU Data Protection Officials on the Use of Cloud Services in Organisations », (2013), SafeGov.org, en ligne : < http://safegov.org/media/53807/safegov.org_report_on_protection_vulnerable_data_subjects.pdf >.

infonuagiques, le contrôle du service est attribué à un administrateur de domaine. Par exemple, dans le cas de Google Apps, l'administrateur de domaine est susceptible de pouvoir :

- afficher les statistiques relatives à votre compte, notamment celles concernant les applications que vous installez;
- modifier le mot de passe de votre compte;
- suspendre ou supprimer l'accès à votre compte;
- accéder aux données conservées dans votre compte et les conserver;
- recevoir les données propres à votre compte pour satisfaire à des obligations légales, réglementaires, judiciaires ou administratives;
- restreindre vos droits de suppression ou de modification des données ou des paramètres de confidentialité.[558]

Or, il va de soi que ces pouvoirs réservés à l'administrateur de domaine peuvent sembler exorbitants pour l'utilisateur final. Cette problématique a récemment été soulevée dans le cadre d'une étude visant la protection des renseignements personnels d'étudiants puisque l'administrateur de domaine sera souvent la direction de l'école et qu'un tel pouvoir pourrait entraîner des abus[559]. Toutefois, ces pouvoirs ne sont pas – à notre avis – aussi problématiques qu'il ne le semble à première lecture puisqu'ils demeurent plus limités que ceux d'un administrateur qui hébergerait lui-même les données. En d'autres mots, l'infonuagique nous semble ici protéger les utilisateurs en limitant les droits de l'administrateur, bien que ceux-ci puissent demeurer très large.

La véritable problématique découlant du rôle d'administrateur de domaine est qu'il appartiendra à ce denier d'accepter les termes d'utilisation du système d'infonuagique visé, rendant ainsi l'acceptation obligatoire pour les utilisateurs. Or, comme le soulève une étude publiée par la CNIL :

---

[558] GOOGLE, « Règles de confidentialité », en ligne : < http://www.google.com/intl/fr/policies/privacy/ >.

[559] « Protecting Vulnerable Data Subjects : Findings from a Survey of EU Data Protection Officials on the Use of Cloud Services in Organisations », préc., note 557.

> « Pour les utilisateurs finaux de Google Apps, l'utilisation d'un Compte Google est décidée par le client de Google Apps (généralement la société employeur des utilisateurs finaux) : le consentement peut donc ne pas être valable. Google devrait appliquer des restrictions à la combinaison de données entre les services et cette combinaison devrait être limitée aux services inclus dans l'offre Google Apps. »[560]

Comme nous l'avons abordé, la gratuité de certains services infonuagiques « logiciels sous forme de service » est liée au fait que l'utilisateur final accepte d'être exposé à certaines publicités. Ces publicités sont choisies par des algorithmes qui analysent les renseignements fournis par les utilisateurs afin de cibler les intérêts exprimés et présumés de ceux-ci en vertu de statistiques relatives aux données collectées (âge, sexe, niveau d'éducation, etc.).

L'utilisateur auquel ce service est imposé par un organisme public se voit donc soumis à une divulgation de ses renseignements personnels à laquelle il n'a pas consenti, et à une utilisation qui diffère de celle pour laquelle le renseignement a été recueilli. Nous sommes donc d'avis que le recours à un service d'infonuagique opérant sous un tel modèle publicitaire serait proscrit par les articles 63.1 et suivants de la *Loi sur l'accès*.

Soulignons par ailleurs que ce modèle d'affaire est d'autant plus problématique si les utilisateurs finaux sont des mineurs. En effet au-delà des risques liés à la confidentialité de données, rappelons que « nul ne peut faire de la publicité à but commercial destinée à des personnes de moins de treize ans »[561]. Ainsi, les écoles et commissions scolaires qui désireraient utiliser un service d'infonuagique tel Google Apps, en plus – évidemment – d'obtenir le consentement des parents puisque les mineurs ne peuvent légalement consentir aux conditions d'utilisation du service[562], devront s'assurer que le modèle de financement du service n'est pas basé sur une quelconque forme de publicité ciblée.

---

[560] CNIL, « Annexe – Règles de confidentialité de Google : principales conclusions et recommandations », (2012), en ligne : < http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/GOOGLE_PRIVACY_POLICY-RECOMMENDATIONS-FINAL-FR.pdf >.

[561] *Loi sur la protection du consommateur*, RLRQ c P-40.1, art. 248.

[562] Outre le fait que l'article 157 C.c.Q. prévoit que « [l]e mineur peut, compte tenu de son âge et de son discernement, contracter seul pour satisfaire ses besoins ordinaires et usuels », et qu'il serait possible de prétendre que le service d'infonuagique n'entre dans ni l'une, ni l'autre de ces catégories, il importe de souligner que le service

- Les risques liés à l'utilisation des logiciels sous forme de service pour les tiers

La question des droits d'accès que se réservent certains services infonuagiques peut aussi avoir des incidences sur certains tiers. En effet, comme nous l'avons énoncé plus haut, bien que l'on puisse être porté à supposer que l'utilisation, par l'employé d'un organisme public, d'un logiciel de traitement de texte dans le nuage n'entraîne aucun risque pour les citoyens, une telle supposition nous apparaît erronée. Par exemple, une lettre adressée à un citoyen contiendra probablement certains renseignements personnels visant celui-ci soit dans son entête (nom et coordonnées postales), soit dans son contenu (données fiscales, NAS, etc.). Bref, même si le service d'infonuagique en question ne vise pas l'hébergement de bases de données sur les citoyens, il donne tout de même accès à certains renseignements confidentiels visant ceux-ci. Évidemment, il est peu probable que Google, pour reprendre cet exemple, lise chacun des documents rédigés en utilisant ses services Google Apps. Ceci étant, tel qu'indiqué plus haut, l'affaire Snowden nous démontre que les ressources pour procéder à une telle analyse existent. Qui plus est, Google a, selon les conditions d'utilisation du site, le droit de procéder à une telle lecture :

> « En soumettant des contenus à nos Services, par importation ou par tout autre moyen, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage ou de distribution public desdits contenus. Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services (par exemple, pour une fiche d'entreprise que vous avez ajoutée à Google Maps). Certains Services vous proposent le

---

Google Apps gratuit n'est pas offert aux enfants de moins de 13 ans : « Google doesn't allow users who are under the age of 13 to have Google Accounts, unless they are using Google Apps for Education accounts through their school ». Notons que le service « Google Apps for education » est un service payant, mais que l'accord des parents demeure nécessaire pour qu'un enfant de moins de 13 ans puisse y avoir accès. Voir le passage d'un communiqué émis par Google cité dans Elizabeth FLOCK, « Father's Open Letter to Google: 'Thanks for Making my Daughter Cry' », (2011) *The Washington Post,* en ligne : < http://www.washingtonpost.com/blogs/blogpost/post/hey-google-thanks-for-making-my-daughter-cry/2011/12/12/gIQAhYx9pO_blog.html >.

> moyen d'accéder aux contenus que vous avez soumis à ce Service et de les supprimer. Certains Services prévoient par ailleurs des conditions ou des paramètres restreignant la portée de notre droit d'utilisation des contenus que vous avez soumis aux Services en question. »[563]

Encore une fois, une telle clause s'avère être incompatible avec les droits des citoyens dont les renseignements personnels pourraient se retrouver dans des documents générés en utilisant le service Google Apps[564]. L'utilisation de tels services gratuits devrait donc être limitée à la préparation de documents statistiques anonymisés ou autres types de documents ne contenant aucun renseignement confidentiel.

Pour clore sur la notion de confidentialité, nous désirons souligner que tout ce qui précède vise l'hébergement, dans le nuage, de documents technologiques contenant des renseignements confidentiels obtenus par un organisme public et dont la collecte et la conservation sont rendues nécessaires ou obligatoires en vertu des obligations dudit organisme. Ainsi, dans les rares cas où un citoyen québécois confie une information confidentielle à un organisme ou Ministère sans y être obligé par un quelconque texte législatif, il sera possible de simplement obtenir le consentement de ce dernier – ou, s'il s'agit d'un mineur, de ses parents ou gardiens – afin que ses renseignements soient hébergés dans le nuage[565].

Pour conclure, il importe de préciser que les incidences juridiques du recours à l'infonuagique par le gouvernement du Québec – notamment en ce qui concerne la responsabilité des divers ministères et organismes qui le composent – dépendront en grande partie du modèle de déploiement envisagé. En effet, si un organisme gouvernemental choisit d'adopter un modèle privé, ou si le gouvernement, dans son ensemble, choisit d'adopter un modèle communautaire sous le contrôle d'un organisme étatique identifié (le CSPQ, par exemple[566]), les rôles et

---

[563] GOOGLE, « Conditions d'utilisation de Google », (2012), en ligne : < http://www.google.com/intl/fr/policies/terms/ >.

[564] *Loi sur l'accès*, art. 63.1 et ss.

[565] *Loi sur l'accès*, art. 53.

[566] Cet exemple correspond à la mise en contexte nous ayant été communiquée lors de la rédaction de la présente étude : « Dans la stratégie infonuagique gouvernementale, la vision du gouvernement est de mettre en œuvre un nuage qui offrira un certain nombre de services infonuagiques aux organismes publics. Il y aura une seule porte

responsabilités de cet organisme seront distincts du cas où le modèle de déploiement implique que l'hébergement de données ou d'applications logicielles soit confié à un tiers situé à l'extérieur de l'administration gouvernementale. D'ailleurs, l'une des questions nous ayant été soumise se réfère à la qualification juridique d'un organisme étatique qui choisit d'héberger des documents technologiques dans le nuage quant à savoir s'il s'agit du « responsable du traitement » (Data controller) ou du « sous-traitant » (Data processor). Cette distinction (responsable du traitement versus sous-traitant) est issue de la *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (ci-après : la « Directive »), laquelle définit les deux rôles ainsi :

- « responsable du traitement » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;

- « sous-traitant »[567] : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement[568].

Transposée en droit québécois, cette distinction est équivalente à celle faite par les articles 25 et 26 de la *LCCJTI*. En effet, rappelons que, en vertu de l'article 25 de la *LCCJTI*, « [l]a personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité », alors que l'article 26 de la même loi prévoit que « [l]e prestataire de services est tenu, durant la période où il a la garde du

---

d'accès au nuage gouvernemental. Le Centre de services partagés du Québec (CSPQ) sera le principal fournisseur/courtier de services infonuagiques ».

[567] La version électronique de la Directive utilise également l'expression « sous-traitement », en ligne : < http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML >.

[568] Article 2 de la Directive. Notons que cette distinction « responsable de traitement » versus « sous-traitant » est maintenue dans la *Proposition de Règlement du Parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données)* en ligne : < http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf >.

document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité ». Bref, le « responsable du traitement » serait « la personne responsable de l'accès », alors que le « sous-traitant » serait le « prestataire de service »[569].

Or, comme que nous l'avons déjà souligné et tel qu'indiqué par Vincent Gautrais et Pierre Trudel :

> « L'accès à des renseignements personnels est assujetti à des limites et il importe de se dissocier de la croyance correspondant à un certain "sens commun" selon laquelle dès lors qu'on est en "possession" physique d'un document, on a le droit d'en prendre connaissance. L'article 25 de la *Loi concernant le cadre juridique des technologies de l'information* réaffirme au contraire que l'obligation de contrôler doit être effectuée par la personne responsable, personne qui n'est pas forcément celle qui gère "physiquement" le document en cause. »[570]

Ainsi, la personne responsable de l'accès à un document technologique sera l'organisme public détenant les renseignements personnels « dans l'exercice de ses fonctions », peu importe qui en assurera la conservation[571]. En d'autres mots, la véritable question juridique est : qui agira en tant que prestataire de service du nuage gouvernemental ? En effet, si l'offre de service infonuagique est assumée par le CSPQ, celui-ci deviendra alors prestataire de services infonuagiques et sera responsable de « voir à ce que les moyens technologiques convenus soient mis en place » pour assurer la sécurité des renseignements personnels hébergés dans le nuage. À l'opposé, si le CSPQ ne joue qu'un rôle consultatif pour identifier des prestataires de services infonuagiques privés avec lesquels un ministère ou organisme pourrait éventuellement signer une entente, sa responsabilité sera écartée en ce qui concerne l'obligation de sécurité[572].

---

[569] Notons que, bien que cela soit extérieur à l'objet de la présente étude, la distinction entre responsable du traitement et sous-traitant implique des obligations au niveau international, notamment en vertu de la Directive. Ainsi, il sera nécessaire d'évaluer ces obligations advenant la signature d'un contrat d'infonuagique avec un prestataire européen.

[570] V. GAUTRAIS et P. TRUDEL, préc., note 514, p. 229.

[571] *Loi sur l'accès*, art. 1.

[572] Ceci n'aura évidemment aucune incidence sur ses autres obligations en vertu de sa loi constitutive. Voir : *Loi sur le centre de services partagés du Québec*, RLRQ c. C-8.1.1.

Confier le rôle de prestataire de services infonuagiques au CSPQ renferme en soi des avantages marqués au niveau de la sécurité des données et de ses incidences juridiques. En effet, rappelons que, en tant qu'organisme public, le CSPQ n'est pas soumis aux formalités administratives prévues au deuxième alinéa de l'article 67.2 de la *Loi sur l'accès*[573]. En d'autres mots, l'organisme public qui aura à confier des renseignements confidentiels au CSPQ n'aura pas à procéder à l'obtention d'engagements de confidentialité de la part de ce dernier. Par ailleurs, un nuage géré par et sous le contrôle du CSPQ obéirait nécessairement au modèle privé interne ou communautaire évitant ainsi les risques juridiques liés à l'extraterritorialité des données et aux droits d'accès du prestataire de services infonuagiques.

Évidemment, procéder de la sorte impliquera un certain nombre d'obligations de la part du CSPQ, puisque ce dernier devra notamment assumer les rôles suivants :

- voir à ce que les moyens technologiques convenus soient mis en place pour préserver l'intégrité des renseignements personnels ou autrement confidentiels;
- voir à ce que les moyens technologiques convenus soient mis en place pour protéger la confidentialité des renseignements personnels ou autrement confidentiels;
- voir à ce que les moyens technologiques convenus soient mis en place pour interdire l'accès à toute personne qui n'est pas habilitée à prendre connaissance des renseignements personnels ou autrement confidentiels;
- assurer le respect de toute autre obligation prévue par la loi relativement à la conservation des renseignements personnels ou autrement confidentiels[574].

Or, il est possible que le CSPQ ne possède pas les moyens, l'espace, ou les effectifs pour assumer toutes ces responsabilités, justifiant ainsi le recours à un ou des prestataires privés. Si cette avenue peut être entièrement justifiée, il importe de noter que le recours à plusieurs prestataires de services infonuagiques distincts pourrait limiter les possibilités de développement de services communs entre les ministères et autres organismes gouvernementaux, allant ainsi à l'encontre de l'un des avantages perçus du recours à l'infonuagique tel que souligné dans les analyses de cas

[573] Il demeure toutefois que, conformément au premier alinéa de ce même article 67.2, le mandat doit être constaté par écrit.

[574] *LCCJTI*, art. 26.

effectuées dans la première partie de la présente étude. Il s'agirait donc de limiter le nombre de prestataires, surtout pour un même modèle de service.

Pour la sélection desdits prestataires de services infonuagiques, la référence à la *Loi sur les contrats des organismes publics*[575] est de mise, notamment pour respecter les obligations du CSPQ telles qu'elles découlent notamment de l'ACI, de l'ACCQO, de l'AQNB 2008 et de l'AQNY[576]. Évidemment, comme nous l'avons déjà souligné, puisque l'ACI « n'a pas pour effet d'obliger une entité à violer les obligations en matière de confidentialité qui lui sont imposées par la loi »[577], le CSPQ pourra, dans le cadre de tout appel d'offres, préciser que l'hébergement des données en sol canadien comporte un avantage comparatif.

B. Le cadre juridique applicable à l'utilisation de l'infonuagique par le gouvernement du Québec : exemples et cas d'application

L'analyse juridique qui précède nous a permis d'identifier les principaux enjeux – notamment en matière de vie privée et de sécurité de l'information – associés au recours, par l'état québécois, à l'infonuagique. Toutefois, cette analyse se voulant générale, il importe d'appliquer les enseignements tirés de celle-ci sur les différents projets d'infonuagique projetés du gouvernement du Québec afin d'avoir une vision plus concrète des incidences du recours à ce type de technologie. Ainsi, quatre cas d'espèce ont été envisagés, à savoir : (1) le gouvernement désire se doter d'une solution en ligne SaaS de Sagir 3; (2) le gouvernement veut connaître les implications liées à l'utilisation d'un système infonuagique de messagerie électronique par ses employés; (3) certains organismes gouvernementaux envisagent d'implanter une plateforme de développement lors de l'élaboration de leurs solutions d'affaires; et (4) le gouvernement entend recourir au service de traitement IaaS pour répondre à des besoins spécifiques.

Tel qu'il nous a été communiqué :

---

[575] Voir *supra*, p. 130.

[576] Voir *supra*, pp. 129 à 131.

[577] ACI, art. 510.

> « les quatre cas d'utilisation proposés pour cette étude ont été retenus après analyse des données recueillies de la Planification triennale des projets et actifs en ressources informationnelles (PTPARI) 2012 et aussi; d'informations obtenues lors de rencontres avec les organismes publics dans le cadre des nombreux ateliers de travail sur différents dossiers. En effet, il en ressort que le recours à l'infonuagique peut être une solution pour plus de vingt (20+) projets identifiés au PTPARI. Ils portent sur l'acquisition et le rehaussement des infrastructures le stockage et le traitement de données ainsi que la mise en place de plateformes de développement. De plus, de nombreux organismes publics ont signifié un intérêt fort pour une solution de courriel à l'échelle gouvernementale. »

Précisons que les menaces liées à la sécurité de l'information seront essentiellement les mêmes et ce, peu importe le modèle de service utilisé[578]. Ainsi, bien que les impératifs techniques diffèrent d'un modèle de service à un autre, les risques juridiques dépendront davantage du modèle de déploiement utilisé par le gouvernement pour l'un ou l'autre de ces services.

Ceci étant, le niveau de contrôle du gouvernement sur les renseignements qu'il détient pourra varier selon le modèle de service qu'il emploie, en corrélation avec le modèle de déploiement utilisé. En outre, les composantes techniques et spécifiques à chaque modèle de service devant être mises en place par le prestataire et, dans certains cas, par l'organisation cliente, auront pour effet de faire varier le niveau de responsabilité incombant au prestataire relativement au système de sécurité[579].

1) La Solution de dotation en ligne SaaS de Sagir 3

a) Description du scénario

« Le CSPQ et Revenu Québec ont fait un appel d'offres conjoint afin d'acquérir une solution de dotation en ligne de type infonuagique. En effet, la solution technologique devra appuyer les changements projetés en matière d'embauche en lien avec l'évolution de la législation, lesquels consistent à revoir et optimiser l'ensemble des étapes du recrutement selon les meilleures pratiques afin d'assurer au gouvernement du Québec et à Revenu Québec une main-d'œuvre en

[578] Voir CLOUD SECURITY ALLIANCE (CSA), « Top Threats to Cloud Computing V1.0 », (2010), en ligne : < https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf >.

[579] Voir TREND MICRO, « Best Practices for Security and Compliance with Amazon Web Services », (2013), en ligne : < http://deepsecurity.trendmicro.com/wp-system/uploads/2013/04/Trend-Micro-Best-Practices-for-Security-and-Compliance-with-Amazon-Web-Services.pdf >, p. 5.

temps opportun et selon les besoins. La solution doit offrir une couverture complète de la dotation tant à l'intérieur qu'à [l'extérieur] du gouvernement. Elle doit soutenir les activités de dotation des emplois pour les quatre modes de dotation : recrutement, promotion, mutation et affectation pour le gouvernement. Elle doit prévoir plusieurs moyens de communication avec les personnes candidats, dans le respect des règles de la confidentialité et de la protection des renseignements personnels, en privilégiant les modes électroniques, par exemple : courriel, formulaires Web, fils RSS, etc.

De plus, l'appel d'offres comprend également une clause d'hébergement qui concerne les renseignements personnels recueillis dans le cadre de la solution de dotation en ligne. Cette clause stipule clairement que les informations doivent être hébergées au Québec et qu'en aucun temps […] ces informations ne pourront être transférées à l'extérieur du Québec à moins que le CSPQ et Revenu Québec soient assurés qu'ils bénéficient d'une protection équivalant à celle prévue à *la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* »[580].

b) Qualification

i) Modèle de service

Le modèle de service choisi pour cette solution de dotation en ligne est le SaaS, tel que décrit plus en détail dans la première section de ce rapport.

ii) Modèle de déploiement

Vu la description du projet, le modèle de déploiement le plus approprié pour une telle solution de dotation en ligne serait le modèle privé externe ou le modèle communautaire, ou encore un modèle hybride de ces deux types de modèles[581]. En effet, la clause d'hébergement qui requiert que les renseignements personnels recueillis dans le cadre de la solution de dotation en ligne soient hébergés au Québec implique l'utilisation de l'un ou l'autre de ces modèles de déploiement puisqu'ils sont les seuls modèles à pouvoir donner aux organismes un véritable contrôle sur

[580] Description nous ayant été remise par le Secrétariat du Conseil du trésor.

[581] Pour une description de ces modèles, voir la Section I-A de la présente étude.

l'emplacement des données. Ceci étant, puisque le service devra être partagé entre deux organismes gouvernementaux, soit le CSPQ et Revenu Québec, l'utilisation d'un modèle communautaire pourrait mieux satisfaire aux besoins décrits.

Même si l'appel d'offres prévoit également la possibilité d'héberger les données dans une autre province ou un autre état dont les lois relatives à la protection des renseignements personnels sont équivalentes à celles du Québec, notre position quant au choix du modèle de déploiement demeure la même puisque le CSPQ et Revenu Québec devront autoriser l'hébergement de ces informations à l'extérieur du Québec suite à une analyse desdites lois. Ces organismes exerceront donc un contrôle continu sur l'emplacement de leurs données, contrôle qui s'avère difficile dans le cadre d'un nuage public.

iii) Caractéristiques du service acquis

Le service acquis sera de la nature d'un logiciel accessible pour toute personne bénéficiant des autorisations requises de la part du CSPQ et/ou de Revenu Québec, moyennant un tarif à l'heure, à l'utilisation (tout dépendant du nombre d'utilisateurs), ou selon la quantité de données stockées. Ce logiciel sera mis à jour régulièrement sans l'intervention du CSPQ ou de Revenu Québec, lesquels n'auront pas à gérer les licences relatives à ce logiciel puisque cette responsabilité sera assumée par le prestataire de services infonuagiques retenu. Le recours au modèle de déploiement privé externe ou communautaire permettra toutefois à ces organisations d'exercer un niveau de contrôle plus élevé sur l'emplacement des données, en plus de bénéficier de l'avantage de l'élasticité des ressources lié à l'infonuagique.

iv) Types de données externalisées

Les renseignements visés sont ceux qui doivent être fournis par une personne qui pose sa candidature pour un poste auprès d'organismes gouvernementaux. Selon le document d'appel d'offres, lequel décrit la solution de dotation en ligne en plus de détail, il serait question de la collecte des renseignements personnels et confidentiels tels que définis par la *Loi sur l'accès*.

Entre autres, les renseignements pouvant être recueillis sont ceux apparaissant au *curriculum vitae* du candidat ainsi que certains renseignements d'affaires[582].

v) Enjeux

Tel qu'il sera discuté plus en détail dans la prochaine section, les principaux enjeux présentés par l'utilisation d'un tel système concernent la sécurité du réseau et des informations qui y seront hébergées, notamment en ce qui concerne l'accès à ces informations par des individus non autorisés.

c) Analyse juridique

L'utilisation d'un modèle privé externe ou d'un modèle communautaire présente certaines problématiques au niveau de la sécurité du réseau. Plus particulièrement, ces modèles imposent l'obligation d'appliquer des mesures de sécurité sur deux périmètres de sécurité, celui du client et celui du prestataire[583]. En ajoutant un périmètre de sécurité, l'on ajoute également une seconde composante susceptible à des attaques externes. Ceci peut donc présenter certains problèmes au niveau juridique, notamment puisqu'une solution de dotation en ligne pour l'embauche implique nécessairement l'hébergement de renseignements personnels sensibles, lesquels renseignements doivent être protégés de la manière prévue par la *Loi sur l'accès*[584] et la *LCCJTI*.

En prévoyant l'utilisation de certaines normes et pratiques pour assurer la sécurité informationnelle, telles que le modèle de gouvernance des TI de CobiT (*Control Objectives for Information and Related Technology*), la norme ISO/IEC 27002, les pratiques ITIL (*Information Technology Infrastructure Library*) et la méthode d'analyse de risques Méhari, l'appel d'offres semble bien répondre à cette obligation[585]. En effet, il importe de rappeler que les mesures de sécurité à mettre en place doivent assurer un niveau de sécurité raisonnable aux données, et non un niveau de sécurité optimal ou parfait (lequel n'est par ailleurs que théorique). Les tribunaux

[582] CENTRE DE SERVICES PARTAGÉS DU QUÉBEC, « Acquisition d'une solution SaaS pour le projet de dotation en ligne Sagir (SGR3): Appel d'offres fondé sur le rapport qualité-prix », article 1.10.

[583] Voir *supra*, p. 22 (inconvénients du modèle privé externe) et p. 26 (inconvénients du modèle communautaire).

[584] Voir *supra*, section II A 3).

[585] CENTRE DE SERVICES PARTAGÉS DU QUÉBEC, préc., note 582.

ont d'ailleurs à maintes reprises accepté le recours à de telles normes pour identifier un niveau de sécurité raisonnable[586] et la *LCCJTI* fait également référence à la possibilité de se fier à « un procédé établi ou à la documentation élaborée par un groupement d'experts »[587] pour établir le niveau de sécurité à mettre en place.

Évidemment, puisque le modèle de service de dotation en ligne prévu par le CSPQ et Revenu Québec prévoit l'accès, par les candidats, à leurs dossiers, un système d'authentification de ces utilisateurs assez sécuritaire doit être créé afin de s'assurer qu'il n'y aura aucun accès non autorisé à ces informations et, ainsi, respecter les exigences des articles 25 et 26 de la *LCCJTI*.

L'utilisation du modèle de service SaaS peut présenter d'autres inconvénients, plus particulièrement parce que l'utilisation de ce service ne serait pas sous le contrôle du CSPQ ou de Revenu Québec. De plus, tel que décrit précédemment[588], certains problèmes peuvent être rencontrés en ce qui a trait au transfert des données via un réseau et au stockage des données de plusieurs utilisateurs dans une application offertes par un même prestataire. Ceci implique que, non seulement le réseau utilisé devra être équipé de technologies de cryptage efficaces, mais également que les données elles-mêmes devront être chiffrées pour assurer leur sécurité. En ce qui concerne la disponibilité du logiciel SaaS, tel qu'expliqué précédemment[589], l'utilisation d'un modèle de déploiement privé externe ou communautaire, bien que plus dispendieux que d'autres modèles de déploiement, augmentera la sécurité et la fiabilité du réseau, respectant, une fois de plus, les obligations d'intégrité et de confidentialité imposées par la *LCCJTI*. Toutefois, pour assurer la disponibilité des données en tout temps, il serait peut être nécessaire, pour le prestataire de service, de générer des copies de sauvegarde des données, ce qui pourra avoir des répercussions au niveau de la fiabilité des informations si les données ne sont pas

[586] Voir par exemple *Delisle* c. *Shawinigan Water & Power Co.*, [1968] R.C.S. 744.

[587] *LCCJTI*, art. 68. Notons que cette disposition vise la reconnaissance de procédés devant être mis en oeuvre pour respecter l'une ou l'autre des obligations imposées par la loi, notamment l'obligation de sécurité prévue à l'article 25 *LCCJTI*.

[588] Voir s*upra*, pp. 34 et ss.

[589] Voir *supra*, p. 34.

synchronisées[590] et, donc, avoir des incidences quant à la possibilité d'utiliser ces données dans l'éventualité d'un litige[591].

Tel qu'énoncé précédemment, le processus d'appel d'offres envisagé pour sélectionner un prestataire, s'il est incontournable vu la valeur projetée d'un tel contrat de service[592], peut toutefois engendrer certains problèmes si le prestataire de services infonuagiques constituant le plus bas soumissionnaire conforme est une entreprise étrangère, où une entreprise dont les serveurs sont situés à l'étranger puisque, selon l'analyse effectuée ci-dessus, le transfert de données confidentielles à l'extérieur du Canada ne respecterait pas les obligations imposées aux ministères et organismes québécois en vertu de la *Loi sur l'accès* et de la *LCCJTI*. Si aucun accord de libéralisation des marchés n'a été conclu avec l'état où l'entreprise est située, un tel scénario peut être évité en prévoyant, dans le cadre de l'appel d'offres, que seules les entités canadiennes qui s'engagent à héberger les données au Canada seront éligibles et, par ailleurs, de prévoir dans le contrat d'hébergement que l'éventuel transfert de données à l'extérieur du Canada, l'acquisition de l'entreprise de prestation de services infonuagiques par des intérêts étrangers ou la fusion de celle-ci avec une entreprise étrangère constituent des cause de résiliation du contrat au bénéfice de l'organisme ou du ministère[593]. Évidemment, dans le cas d'entreprises situées à l'intérieur d'états ayant conclu de tels accords avec le Québec, une telle restriction sera difficile à concilier avec l'esprit des accords et pourrait exposer le CSPQ et Revenu Québec à d'éventuelles contestations judiciaires du processus d'appel d'offres.

2) Le service de courriel gouvernemental (SaaS)

a) Description

« Il est tout à fait envisageable pour le gouvernement du Québec de se doter d'un service de courriel infonuagique gouvernemental. Ce service peut être offert par un fournisseur de solutions infonuagiques comme Google, Microsoft, Telus, Bell, etc. En ce qui a trait aux fournisseurs

[590] Voir *supra*, p. 90.

[591] À cette fin, voir l'article 5 de la *LCCJTI*.

[592] *Loi sur les contrats des organismes publics*, art. 10.

[593] C.c.Q., art. 1604.

Google et Microsoft, ce sont des compagnies américaines dont [le siège social est situé] aux États-Unis. Pour Telus et Bell, ce sont des compagnies canadiennes qui sont soumises *a priori* aux règlementations du Canada. De plus, pour les fournisseurs Google et Microsoft, leurs infrastructures sont à l'extérieur du Canada. Quant à Bell et Telus, il est réaliste de penser que leurs infrastructures de services sont au Canada, mais à l'extérieur du territoire québécois. Enfin, toutes ces compagnies peuvent disposer d'infrastructures de relève délocalisées à l'extérieur du pays, comme aux États-Unis ou en Europe et ailleurs. Enfin, un service de courriel gouvernemental peut contenir tous les types d'information, sensibles et non sensibles. Ces informations parfois confidentielles transitent sur les réseaux de télécommunications publics »[594].

b) Qualification

i) Modèle de service

Selon les informations fournies, le modèle de service retenu pour ce service de courriel gouvernemental serait le modèle SaaS. Tel que nous l'avons expliqué dans la première partie, le logiciel sous forme de service fait référence à l'utilisation d'un logiciel commercialisé en tant qu'application à distance, accessible comme un service, par le biais d'Internet et du Web[595]. Il peut être déployé sur Internet et/ou derrière un pare-feu, sur un espace réseau local ou un ordinateur personnel[596], selon le modèle de déploiement utilisé. Comme nous l'avons vu, les outils de collaboration et autres logiciels offerts en ligne, tels que Google Apps, constituent le modèle de service le plus répandu, tant à l'intérieur qu'à l'extérieur des administrations gouvernementales[597].

ii) Modèle de déploiement

Tous les modèles de déploiement peuvent offrir le logiciel sous forme de service et, par ailleurs, tous les types de données peuvent transiger sur un système de messagerie électronique opérant

---

[594] Description nous ayant été remise par le Secrétariat du Conseil du trésor.

[595] Voir : « SaaS : définition, offre et retours d'expérience », *Journal du net*, en ligne : < http://www.journaldunet.com/solutions/intranet-extranet/saas/ >.

[596] S. SUBASHINI et V. KAVITHA, préc., note 23, 6.

[597] Voir *supra*, p. 32.

dans le nuage, qu'il s'agisse de données publiques, de renseignements personnels et confidentiels, de secrets commerciaux ou de renseignements protégés par droits d'auteur. Toutefois, puisque les informations gouvernementales transmises par courriel doivent « être protégées par un moyen approprié au mode de transmission »[598], il serait souhaitable de recourir à un modèle de déploiement communautaire.

iii) Caractéristiques du service acquis

En utilisant un seul logiciel de système de courriel par le biais d'un modèle de déploiement communautaire, les organismes gouvernementaux en question pourront réduire les coûts liés à la gestion et à la sécurité du système en mettant en commun leurs ressources.

iv) Types de données externalisées

Les données visées sont toutes celles qui pourraient être transmises par courriel par le préposé d'un organisme gouvernemental. Il peut donc s'agir tant de données publiques que de renseignements personnels ou autrement confidentiels. Rappelons que, en ce qui concerne ces derniers types de renseignements, l'article 34 de la *LCCJTI* prévoit ce qui suit :

> **34.** Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication.
>
> La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant.

v) Enjeux

Le principal enjeu d'une telle infrastructure est évidemment d'assurer la sécurité du service de courriel par le biais de contrôles d'accès efficaces. Cela requerra par ailleurs l'adoption de politiques strictes en matière de protection des mots de passe des préposés. Par ailleurs, et tel qu'énoncé dans le descriptif nous ayant été remis, un second enjeu découlant du premier est lié à la situation géographique des serveurs sur lesquels l'information sera hébergée et, donc, à la

[598] *LCCJTI*, art. 34.

portée et à l'effectivité des lois visant à protéger les renseignements personnels disponibles sur ce territoire.

c) Analyse juridique

En vertu du modèle SaaS, les données doivent être collectées chez l'organisation cliente et être transférées via un réseau. Ceci implique donc que le réseau utilisé doit être pourvu de mesures de sécurité efficaces afin de contrer les possibilités d'intrusion et d'assurer un transfert sécuritaire des données sensibles[599]. De plus, un modèle SaaS sécuritaire devrait permettre de savoir où sont localisées les données et d'en informer le client[600].

Nous l'avons vu, même si les prestataires de services infonuagique doivent protéger les renseignements qui leur sont confiés[601], il demeure que les renseignements qui sont situés à l'extérieur du Canada ou sur des serveurs contrôlés par une entité étrangère seront sujets aux lois en vigueur dans le pays hôte. Or, comme les entreprises Google et Microsoft sont états-uniennes, rappelons que le *USA PATRIOT Act* accorde au gouvernement américain de généreux pouvoirs d'accès aux données détenues par une compagnie contrôlée par des intérêts états-uniens ou par une compagnie se trouvant sur le territoire américain[602]. Ainsi, même si les données qui transigent via le service de messagerie du gouvernement sont localisées au Canada, elles peuvent demeurer accessibles pour le gouvernement des États-Unis sous certaines conditions, notamment si une compagnie détient une majorité d'administrateurs américains élus[603].

Tel que nous l'avons exposé plus haut, ce même constat est vrai pour tout état où transigeraient ou seraient hébergés des courriels entre l'État québécois et ses citoyens. Cependant, dans certains

---

[599] Voir L. BADGER *et al.*, préc., note 18, p. 5-5, 5-6. Les types de vulnérabilité relatives à la sécurité des données dans le modèle SaaS peuvent prendre plusieurs formes : Cross-site scripting [XSS], Access control weaknesses, OS and SQL injection flaws, Cross-site request forgery [CSRF], Cookie manipulation, Hidden field manipulation, Insecure storage, Insecure configuration, Network penetration and packet analysis, Session management weaknesses, Insecure SSL trust configuration. Voir également S. SUBASHINI et V. KAVITHA, préc., note 23, 4.

[600] S. SUBASHINI et V. KAVITHA, préc., note 23, 5.

[601] *LCCJTI*, art. 25 et 26.

[602] Voir *supra*, pp. 119 et ss.

[603] Voir *supra*, p. 56.

cas, les lois relatives à la protection des renseignements personnels en vigueur sur un territoire donné pourraient légitimer le recours à l'hébergement en sol étranger en vertu de l'article 70.1 de la *Loi sur l'accès*. C'est le cas, par exemple, des pays de l'Union européenne qui, de l'avis de la Commission européenne, sont substantiellement similaires à la législation en place au Québec et, donc, accorderaient un niveau de protection équivalent aux renseignements contenus dans lesdits courriels[604]. Comme les États-Unis ne possèdent pas de cadre juridique assurant un niveau de protection équivalent à la *Loi sur l'accès* et vu les risques associés au *USA PATRIOT Act*, nous sommes d'avis que le recours aux services de Google ou Microsoft pour le service de courriel proposé serait risqué eu égard aux obligations imposées aux ministères et organismes québécois par la *Loi sur l'accès*. Par contre, il importe de préciser que ces deux entreprises ont choisi d'adhérer aux principes de la sphère de sécurité (Safe Harbour) et que, de ce fait, elles s'engagent à respecter des règles de protection des renseignements personnels qui reprennent les principes mis de l'avant par la Directive 95/46/CE et qui équivaudraient donc, selon une logique transitive, aux exigences de l'article 70.1 de la *Loi sur l'accès*[605]. Or, selon certains auteurs[606], cela viendrait permettre la signature d'ententes avec ces entreprises.

Pour ce qui est des entreprises canadiennes telles que Bell ou Telus, rappelons que, en vertu de la *Loi antiterroriste*[607], le gouvernement canadien dispose de pouvoirs de surveillance similaires à ceux accordés au gouvernement américain par le *USA PATRIOT Act*. En effet, la *Loi antiterroriste* permet à l'État canadien d'investiguer « en vue d'assurer la sécurité nationale et, corrélativement, internationale »[608]. Bref, le risque d'interception des courriels par un gouvernement qui n'est pas celui du Québec demeure réel même si les données sont hébergées ailleurs au Canada (voir même au Québec) et sous le contrôle d'une entreprise canadienne[609].

---

[604] Voir *supra*, p. 115.

[605] EXPORT.GOV, « U.S.-EU Safe Harbor List », en ligne : < http://safeharbor.export.gov/list.aspx >.

[606] J.-F. DE RICO, préc., note 492.

[607] *Préc.*, note 531.

[608] C. CHASSIGNEUX, préc., note 228, à la page 64.

[609] Notons que nous ne connaissons pas la composition des conseils d'administration de ces entreprises. Notre analyse repose donc sur une présomption à l'effet que celles-ci demeurent sous contrôle canadien.

Toutefois, tel que décrit ci haut[610], les lois protégeant les renseignements personnels dans les autres provinces canadiennes ont été jugées comme étant substantiellement similaires à la législation en vigueur au Québec, ce qui porte à croire que, conformément à l'article 70.1 de la *Loi sur l'accès*, la signature d'une entente pour la prestation de services de courriel selon un modèle SaaS avec Bell ou Telus, en supposant que l'information soit hébergée sur le territoire canadien, serait conforme aux exigences de la *Loi sur l'accès*.

Il importe d'évoquer à nouveau qu'une des particularités de l'utilisation d'un modèle SaaS est le manque de contrôle sur les données dont dispose l'organisation cliente ou l'utilisateur[611]. Qui plus est, les hébergeurs de certains logiciels sous forme de service se réservent des droits d'administrateurs de domaine pouvant être incompatibles avec les dispositions de la *Loi sur l'accès*[612].

Afin de protéger la confidentialité des données sensibles, nous sommes donc d'avis que l'utilisation, par le gouvernement du Québec, d'un service de courriel infonuagique opéré par un prestataire de service canadien hébergeant les renseignements au Canada demeure beaucoup moins risquée. Si le gouvernement du Québec doit néanmoins utiliser les services d'un prestataire pour lequel il est impossible de savoir précisément où sont conservées les données, il devra mettre en place certaines mesures de sécurité protégeant les renseignements sensibles contenus dans certains courriels, telles que des technologies de chiffrement[613].

3) Une plateforme de développement et d'intégration (PaaS)

a) Description

« Plusieurs organismes publics pourraient vouloir utiliser une plateforme de développement, d'intégration ou de test en mode infonuagique lors de l'élaboration de leurs solutions d'affaires.

[610] Voir *supra*, p. 114.

[611] Voir *supra*, p. 35.

[612] Voir *supra*, pp. 133 et ss.

[613] Comme nous l'avons vu (voir *supra*, p. 132), l'organisme public se devrait toutefois d'utiliser un service de chiffrement distinct de celui offert par le prestataire de services infonuagiques retenu, sans quoi certains risques pourraient persister, notamment si le prestataire permet à un tiers de prendre copie des renseignements **avant** de procéder au chiffrement des données. Voir : I. THOMSON, préc., note 509.

Ce service pourrait offrir un environnement de développement *Java* par exemple qui permettra aux organismes publics d'accélérer le délai de conception et de mise en œuvre de leurs solutions d'affaires. À cet effet, les organismes publics pourraient déployer et concevoir leurs développements logiciels sur une plateforme d'un prestataire de services infonuagiques de type PaaS. Ils pourraient utiliser les solutions PaaS pour y faire l'essai des nouvelles solutions d'affaires de façon temporaire. Les informations transmises vers ces plateformes de développement seront exécutées, manipulées et traitées dans les délais variables. Les informations stockées peuvent être de natures sensibles ou non. Certaines informations sensibles peuvent également être hébergées à distance pendant la durée du traitement ou de l'essai »[614].

b) Qualification

i) Modèle de service

Le modèle PaaS, aussi appelé « cloud applicatif »[615], a été choisi pour l'accomplissement de ce projet. Ce modèle de service permet un accès aux données via une « plateforme informatique (serveur, dispositif de stockage ou ordinateur) reliée à Internet et hébergée par un opérateur »[616]. Ainsi, le scénario PaaS permettrait aux développeurs du gouvernement de créer des applications exécutables à partir du nuage. D'autre part, et pareillement au modèle SaaS, tous les types de renseignements peuvent être traités lors de son utilisation.

ii) Modèle de déploiement

Vu la description du projet, le modèle de déploiement le plus approprié pour une telle plateforme de développement et d'intégration serait le modèle communautaire. En effet, ce modèle de déploiement nous semble le plus souhaitable pour deux raisons. D'abord, il est possible que certaines informations sensibles soient hébergées dans le nuage. Il est donc préférable de garder le plus de contrôle possible sur le *situs* des serveurs hébergeant ces données, ce qui s'avère plus complexe lorsque l'on recoure au modèle public. Ensuite, certains logiciels seront créés par des

[614] Description nous ayant été remise par le Secrétariat du Conseil du trésor.

[615] « IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », préc., note 115.

[616] P. JOSET, préc., note 12.

employés de l'État, lequel désirera se réserver certains droits de propriété sur ces applications. Or, encore une fois, l'hébergement à l'extérieur du Canada pourrait s'avérer risqué si le territoire hôte d'un serveur n'est pas assujetti à un cadre législatif suffisant en matière de protection des droits d'auteurs. Le modèle hybride est par ailleurs le plus approprié vu la possibilité de collaboration entre les différents organismes publics qui utiliseront ce système. En effet, ce modèle facilitera la communication entre ces organismes et permettra le partage d'applications et d'outils de développement, ce qui serait plus complexe advenant l'adoption de nuages privés par les différents organismes visés.

iii) Caractéristiques du service acquis

L'utilisation d'un tel service donnerait aux organismes gouvernementaux tous les outils nécessaires afin de développer les solutions d'affaires qu'ils envisagent. Les outils seraient hébergés dans le nuage et accessibles via Internet.

iv) Types de données externalisées

Tel qu'indiqué ci-dessus, certaines informations hébergées pourront être de natures sensibles, notamment si les logiciels développés permettent le traitement de renseignements confidentiels. Par ailleurs, les solutions d'affaires ou autres outils développés par le biais de cette plateforme constituent des renseignements industriels, commerciaux, scientifiques, techniques de nature confidentielle au sens de l'article 23 de la *Loi sur l'accès*. Dans un tel cas, il sera nécessaire d'assurer une protection contractuelle à ceux-ci, d'abord pour une raison juridique (notamment s'il s'agit de renseignements communiqués par un partenaire privé), ensuite pour des raisons économiques (pour protéger les investissements du ministère ou de l'organisme, ainsi que sa propriété intellectuelle).

iii) Enjeux

Les enjeux qui sont présentés par ce projet touchent l'intégrité, la disponibilité et la confidentialité des renseignements, ainsi que la protection des droits de propriété intellectuelle des œuvres développées dans ces environnements, tel que décrits plus en détail ci-après.

c) Analyse juridique

Les prestataires de services infonuagique considèrent généralement que les utilisateurs (ou clients) du PaaS disposent d'un plus grand contrôle que le modèle SaaS sur les mesures de sécurité[617]. Ainsi, et tel que mentionné précédemment, un organisme client développant des applications PaaS devra gérer une multitude de risques de sécurité, contrairement à l'utilisation de logiciels SaaS offerts par un prestataire[618].

Rappelons que, en pratique, ce type de modèle poserait surtout des contraintes techniques et opérationnelles[619]. En accédant au réseau de manière intrinsèque, le modèle PaaS nécessite notamment des technologies de chiffrement et les développeurs doivent interagir avec les particularités des navigateurs communs[620].

Tel que nous l'avons mentionné, certains sont d'avis que la réussite d'un tel projet dépend principalement de deux facteurs, soit : les compétences en développement dont dispose l'organisme client et le type d'applications qu'elle souhaite développer dans le PaaS – les deux facteurs étant intimement liés[621].

Soulignons par ailleurs que, outre les autres conditions légales relatives à l'intégrité, à la disponibilité et à la confidentialité des renseignements (tels que déjà abordés dans les cas d'utilisation précédents), les droits de propriété intellectuelle des applications développées par le gouvernement devront être prévus contractuellement[622]. En effet, il n'est pas rare qu'un prestataire de services infonuagiques se réserve certains droits quant aux œuvres déposées sur ses serveurs ou, encore, qu'il exige une licence quant à l'utilisation de celles-ci. Par exemple, la plateforme Google Cloud prévoit que :

---

[617] W. Kuan HON, Christopher MILLARD et Ian WALDEN, « Negotiating Cloud Contracts : Looking at Clouds from Bothsides Now », (2012) 16 *Stan. Tech. L. Rev.* 81, 108.

[618] Voir *supra*, p. 38.

[619] C'est notamment l'avis du NIST. Voir *supra*, page 38.

[620] L. BADGER *et al.*, préc., note 18, p. 6-5.

[621] Voir *supra*, p. 39.

[622] Voir W. K. HON, C. MILLARD et I. WALDEN, préc., note 617, 125.

> « By submitting, posting, generating, or displaying any Application and/or Customer Data on or through the Services, Customer gives Google a worldwide, non-sublicensable, non-transferable, non-exclusive, terminable, limited license to use any Application and/or Customer Data for the sole purpose of enabling Google to provide, maintain, protect, and improve the Services in accordance with the Agreement. »[623]

Qui plus est, tel que discuté ci-dessus, les serveurs d'un prestataire de services infonuagiques pourraient se retrouver à l'intérieur des frontières de pays non signataires de la Convention de Berne[624] et, donc, n'offrant pas de garanties suffisantes en ce qui concerne la protection des droits d'auteur. Ainsi, non seulement sera-t-il nécessaire de prévoir, dans le contrat de service, que les droits de propriété intellectuelle visant tous les logiciels créés et/ou hébergés dans le nuage appartiennent aux organismes qui les ont créés, mais il sera également important de prévoir que ces documents ne pourront être déplacés sur des serveurs situés à l'intérieur des pays qui ne protègent pas les droits d'auteur au même titre que le Canada.

Nous devons toutefois souligner que, même si les applications développées demeurent hébergées sur des serveurs situés en sol canadien, il n'est pas certain qu'elles bénéficieront de la protection de la *Loi sur le droit d'auteur*. En effet, tel que l'a souligné la Cour suprême dans l'arrêt *Théberge* c. *Galerie d'Art du Petit Champlain inc.*[625] : « Un droit d'auteur prend […] naissance dès que l'œuvre est écrite ou autrement attestée sous une forme raisonnablement permanente ("fixée") »[626]. Il est donc nécessaire, pour qu'un document soit qualifié d'œuvre, qu'il soit fixé, c'est-à-dire qu'il soit exprimé sous une forme matérielle quelconque[627]. Or, bien que nous ne soyons pas de cet avis, certains auteurs soumettent que les œuvres hébergées dans le nuage

---

[623] GOOGLE, « Google Cloud Platform Terms of Service », en ligne : < https://developers.google.com/cloud/terms/ >.

[624] *Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886, complétée à PARIS le 4 mai 1896, révisée à BERLIN le 13 novembre 1908, complétée à BERNE le 20 mars 1914 et révisée à ROME le 2 juin 1928, à BRUXELLES le 26 juin 1948, à STOCKHOLM le 14 juillet 1967 et à PARIS le 24 juillet 1971 et modifiée le 28 septembre 1979*.

[625] 2002 CSC 34.

[626] *Id.*, par. 25.

[627] *Canadian Admiral Corp.* c. *Rediffusion Inc.*, [1954] 20 C.P.R. 75, par. 28.

pourraient ne pas être considérées comme respectant cette exigence de permanence[628]. L'absence de certitude à cet égard laisse donc planer certains doutes quant à la protection législative accordée aux œuvres créées et hébergées dans des environnements infonuagiques[629], d'où, une fois de plus, la nécessité pour l'organisme ou le ministère visé de protéger ses droits contractuellement.

Par ailleurs, au cours du téléchargement, de l'hébergement et/ou du traitement des applications crées par un organisme ou ministère, il est possible que le prestataire de services infonuagiques procède à certaines mises à jour ou certains ajustements du système, lesquelles seront également protégés par droit d'auteur. Il pourra donc être difficile de séparer le contenu créé par l'organisme, et les modifications aux outils qui sont la propriété du prestataire. Ceci pourrait notamment être le cas si le développement d'une application par un organisme ou ministère se produit simultanément aux changements effectués à la plateforme par le prestataire de services infonuagiques. It pourra donc, dans certains cas, être difficile d'identifier l'entité qui possède les droits de propriété intellectuelle d'une telle application, plusieurs acteurs ayant contribué à sa création[630].

Finalement, bien qu'une plateforme PaaS puisse être une solution fort intéressante pour le développement d'applications gouvernementales, il importe de tenir compte du cadre juridique incertain relatif à la propriété intellectuelle de telles applications. Ceci étant, bien qu'il soit techniquement possible que les œuvres créées dans le nuage ne remplissent pas les conditions requises pour bénéficier d'une protection en vertu de la *Loi sur le droit d'auteur*, il sera possible de prévoir une protection contractuelle équivalente qui, dans tous les cas s'avère essentielle si les applications sont hébergés à l'intérieur des frontières de pays non signataires de la *Convention de Berne*.

---

[628] Voir : Lisa K. ABE, « Cloud Computing : Copyright Law », (2011), en ligne : < http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/71540bd9-c5d8-4683-8186-2c7ccf2c0f00/Cloud_Computing_Copyright_Law_Mar_31_2011_Lisa_Abe.pdf, p. 9.

[629] *Id.*

[630] ALLEN & OVERY LLP, « Intellectual Property in the Cloud », (2013), en ligne : < http://www.allenovery.com/SiteCollectionDocuments/Intellectual_property_in_the_cloud_May_2013.PDF >.

4) Un service de traitement et de stockage de données (IaaS)

a) Description

« Il est tout à fait pertinent pour le gouvernement de recourir au service de traitement infonuagique, puisque ce dernier offre des opportunités d'économies et d'agilités intéressantes. Le gouvernement via le CSPQ pourrait alors avoir des ententes de services auprès d'un certain nombre de fournisseurs pour former une offre gouvernementale de traitement de données. Ces fournisseurs peuvent ainsi développer des offres infonuagiques en mode public et/ou en mode dédié pour répondre aux besoins du gouvernement. À titre d'exemple, l'Agence du revenu du Québec a utilisé le service de stockage d'Amazon pour la diffusion de vidéoclips dans le cadre de leur programme RESTO. Le ministère du Tourisme met également des vidéoclips promotionnels pour inciter les visiteurs à venir prendre des vacances au Québec. D'autres ministères pourront utiliser les services de traitement et de stockage infonuagique public ou non pour manipuler les données sensibles ou non. De plus, il serait également possible que certains organismes publics exploitent des capacités de traitements des fournisseurs infonuagiques. Pensons au Directeur des élections qui recourent à un fournisseur infonuagique pour augmenter ses capacités de traitement pendant la période de l'élection »[631].

b) Qualification

i) Modèle de service

Le modèle de service choisi pour ce service de traitement et de stockage de données est l'IaaS. Il importe de rappeler que l'infrastructure sous forme de service, aussi appelée « cloud d'infrastructure »[632], est un modèle où l'infrastructure, le réseau et le dispositif de stockage sont offerts par un prestataire. L'infrastructure traditionnellement constituée de serveurs, de postes de travail et d'équipement réseau est désormais mise à la disposition du client par le biais d'Internet

[631] Description nous ayant été remise par le Secrétariat du Conseil du trésor.

[632] « IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », préc., note 115.

et peut être améliorée ou diminuée en fonction des besoins[633]. À l'instar du SaaS et du PaaS, tous les types de données peuvent transiger via le IaaS, selon les besoins visés par le gouvernement.

ii) Modèle de déploiement

Puisque les ministères et organismes visés utiliseront ce service de différentes manières, les modèles de déploiement devront nécessairement varier selon l'utilisation projetée. Dans les cas où l'objectif du projet est le réseautage public ou la diffusion de certaines informations au public (par exemple, le cas de vidéoclips promotionnels pour inciter les visiteurs à venir prendre des vacances au Québec), le modèle public constituera un choix envisageable puisque les informations en question seront disponibles au public, mais gérées par les organismes gouvernementaux les ayant créées. Qui plus est, vu l'aspect public des renseignements contenus, il n'existe aucune obligation de confidentialité obligeant d'exercer un contrôle sur le lieu d'hébergement des données ou sur l'accès à celles-ci. Toutefois, pour les organismes qui entendent utiliser les services de traitement et de stockage infonuagique pour manipuler des données confidentielles, le recours à un modèle de déploiement communautaire (voire même privé) s'avèrera nécessaire afin d'assurer une meilleure protection desdites données.

iii) Caractéristiques du service acquis

Les services acquis comprennent le réseautage, le stockage, les réseaux de distribution de contenu pour améliorer la performance et/ou le coût de servir les clients Web et un service de sauvegarde et de récupération[634]. Ces informations sont mises à la disposition du client par le biais d'Internet et peuvent être améliorées ou diminuées en fonction des besoins[635]. Le client ne gère pas l'infrastructure infonuagique sous-jacente, mais il exerce un contrôle sur les systèmes d'opération et le stockage.

---

[633] M. TREMBLAY, préc., note 15.

[634] L. BADGER *et al.*, préc., note 18, p. 6-1.

[635] M. TREMBLAY, préc., note 15.

Toutefois, si le modèle de déploiement utilisé est le modèle public, le traitement des données aura lieu à l'extérieur du coupe-feu de l'organisation[636]. De plus, le modèle public est caractérisé par une réduction des coûts, une augmentation de l'efficience[637] et ne comporte généralement pas de restrictions quant aux capacités de localisation et de stockage. Au contraire, si le modèle de déploiement utilisé est le modèle communautaire, les ressources informatiques seront fournies exclusivement aux organismes détenant des buts et politiques similaires.

iv) Types de données externalisées

Les données visées par ce projet sont variées et dépendront de l'organisme ou du ministère visé. Ainsi, certaines données seront de nature publique et ne nécessiteront aucune protection particulière (par exemple, les informations partagées sur les réseaux sociaux ou des vidéoclips promotionnels), alors que d'autres seront de nature confidentielle.

v) Enjeux

Les enjeux du présent projet sont associés aux caractéristiques des données qui seront traitées ou conservées par le biais du service.

c) Analyse juridique

Comme nous l'avons vu, l'adoption du modèle IaaS par le gouvernement lui offrirait une plus grande marge de manœuvre et une meilleure flexibilité, en lui permettant de faire migrer tout type d'application existante et de déplacer le contenu de ses serveurs dans le nuage. Par conséquent, le gouvernement se libèrerait de la nécessité de posséder (gérer, maintenir et contrôler, etc.) ses propres serveurs et autres infrastructures de traitement de données. Ainsi, ceci lui permettrait notamment de réduire ses coûts (coûts d'acquisition, de maintenance et de recyclage de ses équipements)[638]. Notons que l'utilisation du IaaS requiert des connaissances

---

[636] Aussi dénommé « pare-feu », un « coupe feu » est défini comme étant un « dispositif informatique qui permet le passage sélectif des flux d'information entre deux réseaux, ainsi que la neutralisation des tentatives de pénétration extérieures ». Voir : OLF, préc., note 3.

[637] W. JANSEN et T. GRANCE, préc., note 27, p. 6.

[638] « IaaS, PaaS et SaaS avantages et inconvénients », *préc.*, note 158. Voir également « Cloud computing le concept », préc., note 154.

techniques particulières. Plus spécifiquement, l'utilisation de certains services d'Amazon nécessiterait des compétences avancées en développement d'applications[639].

En outre, l'utilisation du modèle IaaS comporte une particularité importante : l'organisation cliente possède un droit de regard sur la configuration du système et dispose ainsi d'un plus grand contrôle sur celui-ci. Selon les conclusions d'une étude de la Stanford University, l'utilisation du modèle IaaS engendre donc une responsabilité partagée entre le prestataire de services infonuagiques et l'organisation cliente :

> « Providers such as Amazon stress that cloud involves shared responsibility: both users and providers have responsibility for data integrity, backup and security, and allocation of responsibilities and risks needs careful consideration. Users generally have more control with IaaS or PaaS than with SaaS, because IaaS users instantiate or terminate virtual servers and choose what to install on those servers, such as firewalls, anti-malware and other security measures; and users decide what applications they wish to install and host on IaaS or PaaS, such applications often being user-developed and therefore user-controlled. In contrast, SaaS users use standardized applications, provided by SaaS providers in environments which users cannot control, relying on providers to secure applications as well as environments. »[640]

En l'occurrence, ceci ne pose pas problème en ce qui a trait aux données partagées sur les réseaux sociaux ou aux vidéoclips promotionnels. Toutefois, pour ce qui est des données sensibles qui peuvent être hébergées dans le nuage, le fait que l'intégrité et, plus largement, la sécurité, pourraient être compromises sera problématique au niveau juridique, notamment en ce qui concerne les exigences mises de l'avant par les articles 25 et 26 de la *LCCJTI* que nous avons analysés ci-dessus. Bref, l'hébergement de données confidentielles sur les serveurs d'un prestataire tel Amazon n'offrirait pas de garanties sécuritaires suffisantes en vertu des articles précités, ainsi que des autres dispositions analysées dans le cadre de la présente étude.

---

[639] « Amazon does require sophisticated application development skills and does not enable users to quickly get up and running without advanced technical know-how ». Voir « Demystifying SaaS, PaaS, and IaaS », (2011) *Skytap*, en ligne : < http://www.skytap.com/blog/demystifying-saas-paas-and-iaas >. Voir également TREND MICRO, préc., note 579.

[640] W. K. HON, C. MILLARD et I. WALDEN, préc., note 617, 95.

En ce qui a trait aux autres types de données, en plus des conditions liées au transfert des renseignements, un contrat conclu entre le gouvernement et un prestataire de services IaaS devrait prévoir les responsabilités incombant à chaque partie[641]. De plus, le contrat devrait tenir compte des risques liés aux interactions non désirées entre les différents clients du prestataire de services infonuagiques et, de ce fait, prévoir que le réseau IaaS sera en mesure d'empêcher qu'un utilisateur accède à certains blocs de données (« packets ») envoyés dans le système par les utilisateurs d'une autre organisation cliente[642], plus particulièrement en ce qui concerne les blocs de données transmettant des informations sensibles. En raison des problèmes de dépendance au réseau évoqués dans la première partie de la présente étude, le prestataire devrait par ailleurs garantir que les utilisateurs du service pourront disposer d'une bande passante suffisante[643]. Ceci sera toutefois un problème moins inquiétant en ce qui concerne les informations publiques ou non sensibles.

Rappelons finalement que la responsabilité de gérer les identités pour accéder au service IaaS incombera généralement au client[644]. Ainsi, toutes les questions liées aux mesures d'authentifications relevant de la responsabilité du gouvernement devraient être prévues, en plus des conditions de sécurité et d'audits, des droits de propriété intellectuelle et des modalités de gestion des incidents pouvant survenir dans le système IaaS[645]. Cela s'avère nécessaire non seulement afin de garantir la disponibilité des informations confidentielles, mais également l'accessibilité des informations publiques, puisque l'accès au service IaaS donnera aux préposés de l'organisme le pouvoir de changer ou de modifier les données en question.

---

[641] C'est notamment ce qui est prévu à l'article 26 de la *LCCJTI*.

[642] Voir *supra*, p. 42.

[643] *Id.*

[644] Voir *supra*, p. 41.

[645] Voir W. K. HON, C. MILLARD et I. WALDEN, préc., note 617.

CONCLUSION

Conclure une étude comme celle-ci s'avère être une tâche relativement complexe puisque la relative nouveauté de l'infonuagique n'offre pas suffisamment de recul pour permettre d'identifier avec clarté comment l'industrie réagira aux différentes problématiques identifiées. En effet, l'infonuagique est un paradigme en constante évolution, « [i]ts definitions, use cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time »[646]. Ainsi, les révélations découlant de l'affaire Snowden et les récriminations faites aux autorités américaines par différents chefs d'États européens à la suite de celles-ci portent à croire que les États-Unis devront éventuellement modifier leurs comportements s'ils désirent maintenir leur position géopolitique, ce qui risque de nous forcer à réévaluer les risques associés à l'hébergement de données en sol américain. De leur côté, les prestataires de service ayant collaboré avec les autorités états-uniennes devront réviser leurs modèles d'affaire afin de répondre aux exigences de leurs clientèles internationales. Bref, les contraintes tant juridiques, qu'informatiques, que géopolitiques de l'infonuagique risquent d'évoluer rapidement au cours des prochaines années.

Dans l'immédiat, toutefois, les ministères et organismes québécois qui désirent migrer leurs données vers le nuage doivent prendre en compte le contexte juridique et géopolitique actuel. Or, selon notre interprétation du cadre juridique québécois ou, de façon plus spécifique, de la *Loi sur l'accès* et de la *Loi concernant le cadre juridique des technologies de l'information*, il ne serait simplement pas possible d'héberger, de traiter, ou de faire circuler des données confidentielles dans un nuage dès lors que l'un ou l'autre des serveurs qui le composent est situé à l'extérieur du Canada ou est sous le contrôle d'une entité étrangère. Cette interprétation repose tant sur la lettre de la loi, que des échanges intervenus en commission parlementaire, que d'une analyse des principales positions doctrinales et jurisprudentielles. Ainsi, selon notre analyse, l'idéal, afin de respecter les obligations législatives imposées aux ministères et organismes québécois, serait la mise en place d'un nuage privé interne ou communautaire gouvernemental, qui permettrait à la

[646] P. MELL et T. GRANCE, préc., note 8.

fois un partage de certaines informations et de certains services entre les organismes publics, tout en assurant le niveau de sécurité requis. Si cela s'avère impossible, il demeure préférable de favoriser l'hébergement au Canada ou, si cela s'avère impossible, dans les pays européens, vu la similitude des textes de loi relatifs à la vie privée dans ces pays et au Québec.

Nous admettons toutefois d'emblée que ce modèle d'affaire n'est simplement pas réaliste vu le contexte économique actuel. En effet, le principe même de l'infonuagique implique le maintien de plusieurs serveurs sur divers territoires. Ainsi, si le gouvernement québécois désire bénéficier des avantages économiques offerts par l'infonuagique, il s'avère quelque peu illogique d'exclure tout modèle de déploiement qui viendrait réduire un nuage à un simple contrat d'hébergement. Dans tous les cas, vu la mondialisation des marchés et la fusion ou le rachat de sociétés canadiennes avec ou par des compétiteurs internationaux, le nombre d'hébergeurs locaux risque d'être de plus en plus restreint et les entreprises « 100 % canadiennes » de moins en moins compétitives au niveau international. Il s'avèrera donc difficilement justifiable, du stricte point de vu financier, de payer un prix supérieur pour le même service. Qui plus est, même si cela s'avère préférable, vu les questions de sécurité énoncées, il demeure que, tel que nous l'avons invoqué, le Québec est signataire d'ententes interprovinciales et internationales qui limitent son pouvoir discrétionnaire dans le choix d'éventuels prestataires de service d'infonuagique rendant tout traitement préférentiel de prestataires de services québécois ou canadiens problématique. Finalement, soulignons que, même si toutes ces contraintes étaient inexistantes, certaines ententes internationales liant le Québec nécessitent le transfert de données confidentielles à l'extérieur de la province, peu importe ce qui est prévu dans les différents textes de loi en vigueur.

En effet, sans vouloir tomber dans le cynisme, il nous faut souligner le fait que les informations contenues dans des nuages locaux demeurent susceptibles d'être interceptées par (ou communiquées à) des autorités étrangères, notamment parce que le gouvernement canadien aurait signé des ententes de collaboration internationales liées à la lutte contre le terrorisme avec ces pays[647], ou simplement parce qu'il est possible pour des gouvernements étrangers d'exploiter les failles de sécurité de systèmes présumés sécuritaires. Par exemple, certains commentateurs

[647] J.-F. De RICO, préc., note 492.

prétendent que les pirates informatiques qui auraient eu accès aux serveurs du gouvernement canadien en 2012 étaient financés par le gouvernement chinois, bien qu'aucune preuve de telles accusations n'ait été communiquée au public[648].

Ainsi, puisqu'il s'avère difficile, certains diraient même impossible, de respecter la lettre de la loi, nous sommes d'avis que les ministères et organismes qui décident de migrer vers une infrastructure incorporant l'infonuagique devraient tout au moins tenter d'en respecter l'esprit en procédant au chiffrement des données confidentielles hébergées, traitées ou circulant dans le nuage. Une telle pratique, si elle ne viendrait pas empêcher le prestataire de détenir les données, l'empêcherait toutefois de les consulter ou de les partager. De ce fait, cette pratique, si elle ne correspond pas aux exigences de sécurité imposées par la *Loi sur l'accès*, viendrait assurer une plus grande protection aux données confidentielles qu'une politique protectionniste favorisant l'hébergement en sol québécois tel qu'il est prévu à l'article 70.1 de la *Loi*. Il nous faut toutefois souligner qu'opter pour une telle solution nécessite une analyse préalable du cadre juridique applicable au chiffrement des données. En effet, la *Loi concernant le cadre juridique des technologies de l'information* contient un certain nombre de dispositions qui encadrent et limitent les choix technologiques envisageables si l'État québécois en venait à opter pour une solution de chiffrement des données contenues dans le nuage. Bien que l'analyse de ces dispositions et des technologies visées dépasse le cadre de la présente étude, elle s'avère essentielle avant de procéder à une quelconque communication ou transmission de renseignements confidentiels dans un nuage hébergé à l'étranger.

Finalement, peu importe le cadre législatif applicable, il demeure que l'hébergement de données dans le nuage nécessite la rédaction de clauses contractuelles prévoyant la confidentialité des données confidentielles hébergées[649], les mesures de sécurité à mettre en place le cas échéant[650], les droits de propriété intellectuelle du gouvernement sur les contenus hébergés et, surtout, les

[648] David LJUNGGREN, « Canada won't say if China Involved in Hacking Incident », (2012) *Reuters*, en ligne : < http://www.reuters.com/article/2012/09/28/net-us-hacking-idUSBRE88R0N720120928 >.

[649] *Loi sur l'accès*, art. 67.2.

[650] *LCCJTI*, art. 26.

gestes que ne peut poser le prestataire de service à l'égard des documents lui ayant été confiés (transférer les données à l'extérieur du pays, les partager avec des tiers, en garder copie, etc.).

RÉFÉRENCES

Bibliographie

Monographies

BARIBEAU, Marc, Sylvain GADOURY et Patrick GINGRAS, *Principes généraux de la Loi sur le droit d'auteur*, Québec, Publications du Québec, 2013.

BAUER, Eric et Randee ADAMS, *Reliability and Availability of Cloud Computing*, 1re éd., Hoboken, John Wiley & Sons, Inc., 2012.

CHASSIGNEUX, Cynthia, *Vie privée et commerce électronique*, Montréal, Thémis, 2004.

CÔTÉ, Pierre-André, *Interprétation des lois*, 4e éd., Montréal, Thémis, 2009.

DORAY, Raymond et François CHARETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Yvon Blais, 2001.

FAIRBAIRN, Keith G. et Julie A. THORBURN, *Law of Confidential Business Information*, Aurora, Canada Law Book, 2006.

GAUTRAIS, Vincent et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Thémis, 2010.

GAUTRAIS, Vincent, *Preuve technologique*, Montréal, Lexis Nexis, 2014.

HUBIN, Joël et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur, Crid, 1998.

REID, Hubert, *Dictionnaire de droit québécois et canadien*, 4e éd., Montréal, Wilson & Lafleur, 2010.

RHOTON, John, David GRAVES et Jan DE CLERCQ, *Cloud Computing Protected*, USA, Recursive Press, 2013.

ROMPRÉ, Sophie, *La surveillance de l'utilisation d'Internet au travail*, Cowansville, Yvon Blais, 2009.

SAYEGH, F. Georges, Les secrets de commerce et les renseignements confidentiels, Cowansville, Yvon Blais, 2006.

TIPTON, Harold F. et Micki KRAUSE, *Information Security Management Handbook*, 6e éd., Boca Raton, Auerbach Publications, 2007.

VERMEYS, Nicolas W., *Responsabilité civile et sécurité informationnelle*, Cowansville, Yvon Blais, 2010.

Articles de revues ou d'ouvrages collectifs

BICH, Marie-France, « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans *Développements récents en droit de la propriété intellectuelle*, Cowansville, Yvon Blais, 2003, p. 243.

BROWNE, Peter S., « Computer Security – A Survey », (1972) 4(3) *Database* 1.

CHASSIGNEUX, Cynthia, « Quand la sécurité nationale interpelle la protection des renseignements personnels : l'exemple de la *USA Patriot Act* », dans Service de la formation continue du Barreau du Québec, *Vie privée et protection des renseignements personnels (2006)*, Cowansville, Yvon Blais, 2006, page 61.

DE RICO, Jean-François, « L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements », (2014) 6 *Technologies de l'information en bref* 2.

DELWAIDE, Karl, « Quebec Privacy Law Poses Difficulties for Outsourcing of Personal Information », (2007) 27 *Lawyers Wkly* 14.

DUBOIS, Martin, « Nouvelles technologies de l'information et des communications et sécurité informationnelle », dans Service de la formation permanente du Barreau du Québec, *Développements récents en droit de l'accès à l'information (2002)*, EYB2002DEV565.

DUSSAULT, Yves D., « Modifications au régime de protection des renseignements personnels », (2006) *Repères* EYB2006DEV1265.

FABIEN, Claude , « La preuve par document électronique », (2004) 38 *R.J.T.* 533.

HON, W. Kuan, Christopher MILLARD et Ian WALDEN, « Negotiating Cloud Contracts : Looking at Clouds from Bothsides Now », (2012) 16 *Stan. Tech. L. Rev.* 81.

LACHAPELLE, Éric et René ST-GERMAIN, « Protection des actifs informationnels », dans Abdelhaq ELBEKKALI, *Gouvernance, audit et sécurité des TI*, Brossard, CCH, 2008, p. 315.

MARSTON, Sean, *et al.*, « Cloud Computing – The Business Perspective », (2011) 51 *Decision Support Systems* 176.

NIED, Matthew, « Cloud Computing, the Internet, and the *Charter* Right to Privacy : The Effect of Terms of Service Agreements on Reasonable Expectations of Privacy », (2011) 69(5) *The Advocate* 701.

PAQUETTE, Scott, Paul T. JAEGER et Susan C. WILSON, « Identifying the Security Risks associated with Governmental Use of Cloud Computing », (2010) 27 *Government Information Quarterly* 245.

SUBASHINI, S. et V. KAVITHA, « A Survey on Security Issues in Service Delivery Models of Cloud Computing », (2011) 34 *Journal of Network and Computer Applications* 1.

ZISSIS, Dimitrios et Dimitrios LEKKAS, « Securing e-Government and e-Voting with an Open Cloud Computing Architecture », (2011) 28 *Government Information Quarterly* 239.

Documents technologiques

« Accords de libéralisation des marchés publics : seuils d'application » : http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/accords/tab_synthese_seuils_accords.pdf.

« Assujettissement aux accords de libéralisation des marchés publics : ministères et organismes du gouvernement ou de l'assemblée nationale » : http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/accords/tab_synthese_assujettissement_accords.pdf.

« Cloud computing le concept », *Cloud Computing* : http://cloudcomputing.fr/laas-paas-saas.php.

« Demystifying SaaS, PaaS, and IaaS », (2011) *Skytap* : http://www.skytap.com/blog/demystifying-saas-paas-and-iaas.

« Digital Britain Commits Government to Cloud Computing », (2009) *Computing* : http://www.computing.co.uk/ctg/news/1816113/digital-britain-commits-government-cloud-computing.

« IaaS, PaaS et SaaS avantages et inconvénients », (2012) *Yes We Cloud* : http://www.yeswecloud.fr/cloud/iaas-paas-et-saas-avantages-et-inconvenients-629.html.

« IaaS, SaaS et PaaS: les trois grands modèles de service du cloud », (2011) *L'informaticien* : http://www.linformaticien.com/dossiers/id/20578/iaas-paas-et-saas-les-trois-grands-modeles-de-service-du-cloud.aspx.

« L'Approche Platform as a Service (Paas) », (2011) *01 Business* : http://pro.01net.com/editorial/520437/lapproche-platform-as-a-service-%28paas%29/.

« SaaS : définition, offre et retours d'expérience », *Journal du net* : http://www.journaldunet.com/solutions/intranet-extranet/saas/.

« Synthèse des accords de libéralisation des marchés publics : Ministères et organismes du gouvernement » : http://www.tresor.gouv.qc.ca/fileadmin/PDF/faire_affaire_avec_etat/cadre_normatif/accords/tab_synthese_internet_mo.pdf.

ABE, Lisa K., « Cloud Computing: Copyright Law », (2011) : http://www.fasken.com/files/Event/3195cb2b-f29b-456d-8f98-7a3175930523/Presentation/EventAttachment/71540bd9-c5d8-4683-8186-2c7ccf2c0f00/Cloud_Computing_Copyright_Law_Mar_31_2011_Lisa_Abe.pdf.

ACCENTURE, « Cloud Computing and Sustainability : The Environmental Benefits of Moving to the Cloud », (2010) : http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Sustainability_Cloud_Computing_TheEnvironmentalBenefitsofMovingtotheCloud.pdf.

ALLEN & OVERY LLP, « Intellectual Property in the Cloud », (2013) : http://www.allenovery.com/SiteCollectionDocuments/Intellectual_property_in_the_cloud_May_2013.PDF.

ARMHURST, Michael, *et al.*, « Above the Clouds : A Berkely View of Cloud Computing », (2009) : http://www.cs.columbia.edu/~roxana/teaching/COMS-E6998-7-Fall-2011/papers/armbrust-tr09.pdf.

AUSTRALIAN GOVERNMENT DEPARTMENT OF DEFENCE INTELLIGENCE AND SECURITY, « Cloud Computing Security Considerations », (2012) : http://www.dsd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf.

AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE, « Negotiating the Cloud – Legal Issues in Cloud Computing Agreements » (2013) : http://agict.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf.

BADGER, Lee, Tim GRANCE, Robert PATT-CORNER et Jeff VOAS, « Cloud Computing Synopsis and Recommendations », (2012) *NIST* : http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075.

BEIZER, Doug, « USA.gov will Move to Cloud Computing », (2009) : http://fcw.com/articles/2009/02/23/usagov-moves-to-the-cloud.aspx.

BODLE, Irene, « SaaS Agreements – SaaS, PaaS, IaaS – Is There a Difference ? », (2012) *Bodle Law* : http://www.bodlelaw.com/saas/saas-agreements-saas-paas-iaas-is-there-a-difference.

CABINET OFFICE, « Government ICT Strategy », (2011) : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85968/uk-government-government-ict-strategy_0.pdf.

CANELLOS, David, « Adopting the Cloud While Adhering to Domestic & Foreign Government Regulations », (2013) : http://safegov.org/2013/10/2/adopting-the-cloud-while-adhering-to-domestic-foreign-government-regulationsCAVOUKIAN, Ann, « Privacy in the Clouds », (2008) : http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf.

CLOUD SECURITY ALLIANCE (CSA), « Top Threats to Cloud Computing V1.0 (2010) : https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

CNIL,

« Annexe – Règles de confidentialité de Google : principales conclusions et recommandations », (2012) : http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/GOOGLE_PRIVACY_POLICY-RECOMMENDATIONS-FINAL-FR.pdf.

« Carte des autorités de protection des données dans le monde » : http://www.cnil.fr/linstitution/international/les-autorites-de-controle-dans-le-monde/.

« Le panorama des législations », (2008) : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/panorama-legislation.pdf.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA,

« Introduction à l'infonuagique » : http://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_f.pdf.

« La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) », (2013) : http://www.priv.gc.ca/leg_c/leg_c_p_f.asp.

« Lois provinciales essentiellement similaires à la loi fédérale » : http://www.priv.gc.ca/leg_c/legislation/ss_index_f.asp.

« Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique », (2011) : http://www.priv.gc.ca/resource/consultations/report_201105_f.pdf, p. 47.

« Traitement transfrontalier des données personnelles : Lignes directrices », (2009) : https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.pdf.

« Visez les nuages : Questions liées à la protection de la vie privée dans le contexte de l'informatique dans les nuages », (2010) : http://www.priv.gc.ca/information/research-recherche/2010/cc_201003_f.asp#ftnref6.

CURTIS, Sophie, « Forrester : The Cloud Is Inherently Green », (2011) : http://www.techweekeurope.co.uk/news/forrester-the-cloud-is-inherently-green-33331.

DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS, « Building Britain's Digital Future », (2009) : http://webarchive.nationalarchives.gov.uk/20090930121249/bis.gov.uk/building-britains-digital-future#.

DEPARTMENT FOR CULTURE, MEDIA and SPORT AND DEPARTMENT FOR BUSINESS, INNOVATION AND SKILLS, « Digital Britain : The Final Report », (2009) : http://webarchive.nationalarchives.gov.uk/+/http:/www.culture.gov.uk/images/publications/digitalbritain-finalreport-jun09.pdf.

EMC^2,

« Créer un cloud sécurisé : stratégies de déploiement des clouds privés et hybrides » : http://france.emc.com/collateral/emc-perspective/h8558-cloud-trust-ep.pdf, p. 6.

« Le cloud privé et ses avantages métiers : des coûts réduits et une réactivité accrue », (2010) : http://france.emc.com/collateral/emc-perspective/h6870-consulting-cloud-ep.pdf.

EXPORT.GOV, « U.S.-EU Safe Harbor List » : http://safeharbor.export.gov/list.aspx.

FISCHER, Eric A. et Patricia MOLONEY FIGLIOLA, « Overview and Issues for Implementation of the Federal Cloud Computing Initiative : Implications for Federal Information Technology Reform Management », (2013) : http://www.fas.org/sgp/crs/misc/R42887.pdf.

FLOCK, Elizabeth, « Father's Open Letter to Google : 'Thanks for Making my Daughter Cry' », (2011) *The Washington Post* : http://www.washingtonpost.com/blogs/blogpost/post/hey-google-thanks-for-making-my-daughter-cry/2011/12/12/gIQAhYx9pO_blog.html.

GARTNER, « IT Glossary » : http://www.gartner.com/it-glossary/software-as-a-service-saas/.

GLOBAL ACCESS PARTNERS, « GAP Task Force on Cloud Computing », (2011) : http://www.globalaccesspartners.org/Cloud-Computing-GAP-Task-Force-Report-May-2011.pdf.

GOOGLE,

« Conditions d'utilisation de Google », (2012) : http://www.google.com/intl/fr/policies/terms/.

« Google Cloud Platform Terms of Service » : https://developers.google.com/cloud/terms/.

« Privacy Policy » : http://www.google.com/intl/en/policies/privacy/.

« Règles de confidentialité », http://www.google.com/intl/fr/policies/privacy/.

GOVERNMENT OF AUSTRALIA, DEPARTMENT OF FINANCE AND DEREGULATION, « Cloud Computing Strategic Direction Paper : Opportunities and Applicability for Use by the Australian Government », (2013) : http://agimo.gov.au/files/2012/04/final_cloud_computing_strategy_version_1.pdf, p. 28.

GOVERNMENT OF SASKATCHEWAN,

« An Overarching Personal Information Privacy Framework for executive Government », (2003) : http://www.publications.gov.sk.ca/redirect.cfm?p=32639&i=39659.

« The Career Centre » : www.careers.gov.sk.ca/.

HM GOVERNMENT,

« Government Cloud Strategy », (2011) : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf.

« Government ICT Strategy – Strategic Implementation Plan », (2011) : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/266169/govt-ict-sip.pdf.

INSITITUT CANADIEN DES COMPTABLES AGRÉÉS, « Infonuagique : les grandes tendances technologiques », (2012) : http://www.icca.ca/champs-dexpertise/gestion-de-linformation-et-technologies-de-linformation/les-grandes-tendances-technologiques/item72208.pdf.

JANSEN, Wayne et Timothy GRANCE, « Guidelines on Security and Privacy in Public Cloud Computing », (2011) NIST : http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

JOSET, Patrick, « Cloud Computing, tentative de définition », (2011) *Abissa Informatique* : http://www.abissa.ch/data/fichiers/tec_cloud_computing.pdf.

JOURNAL DU NET, « SaaS : définition, offre et retours d'expérience » : http://www.journaldunet.com/solutions/intranet-extranet/saas/.

KLEIN, Kris, « Clarification de l'application du droit canadien de la protection des renseignements personnels au transfert transfrontalier de ces renseignements du Canada vers les États-Unis », (2008) *Industrie Canada* : http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/Clarification%20de%20l%E2%80%99application%20du%20droit%20canadien%20de%20la%20protection%20des%20renseignements%20personnels.pdf/$file/Clarification%20de%20l%E2%80%99application%20du%20droit%20canadien%20de%20la%20protection%20des%20renseignements%20personnels.pdf.

KLINE WEINRICH, Nedra, « The CDC's Second Life », (2006) : http://blog.social-marketing.com/2006/11/cdcs-second-life.html.

KUNDRA, Vivek, « Federal Cloud Computing Strategy », (2011) : https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf.

LIEBENAU, Jonathan, Patrik KARRBERG, Alexander GROUS et Daniel CASTRO, « Modelling the Cloud », (2012) *LSE* : http://www.lse.ac.uk/businessAndConsultancy/LSEEnterprise/news/2012/cloud.pdf.

LIPOWICZ, Alice, « Living NOAA's Second Life », (2009) : http://fcw.com/Articles/2009/03/23/Eric-Hackathorn-NOAA.aspx.

LJUNGGREN, David, « Canada Won't Say if China Involved in Hacking Incident », (2012) *Reuters* : http://www.reuters.com/article/2012/09/28/net-us-hacking-idUSBRE88R0N720120928.

MARK, Roy, « Do Federal Agencies Belong in Cloud Computing Networks ? », (2008) : http://www.eweek.com/c/a/Government-IT/Should-Feds-Climb-on-the-Cloud/.

MELL, Peter et Timothy GRANCE, « The NIST Definition of Cloud Computing », version 15 : http://csrc.nist.gov/groups/SNS/cloud-computing/.

MICROSOFT, « Informations sur les conditions d'utilisation », (2012) : http://www.microsoft.com/france/core/copyright.aspx.

O'HARA, Colleen, « Virtual Learning Gets Second Wind from Second Life », (2009) : http://fcw.com/articles/2009/05/04/feature-virtual-learning.aspx.

OEFFNER, Kevin M., « e-Filing Update », (2006) : http://www.oakgov.com/courts/circuit/Documents/laches/june-06-laches-c.pdf.

OFFICE DE LA LANGUE FRANÇAISE, *Grand dictionnaire terminologique* : http://www.granddictionnaire.com.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FOR BRISTISH COLUMBIA,

« Cloud Computing Guidelines for Public Bodies », (2012) : https://www.oipc.bc.ca/guidance-documents/1427.

« Privacy and the USA Patriot Act, Implications for British Columbia Public Sector Outsourcing », (2004) : http://www.oipc.bc.ca/special-reports/1271.

SAFEGOV.ORG, « Protecting Vulnerable Data Subjects : Findings from a Survey of EU Data Protection Officials on the Use of Cloud Services in Organisations », (2013) : http://safegov.org/media/53807/safegov.org_report_on_protection_vulnerable_data_subjects.pdf.

STODDART, Jennifer, « Pouvoirs de surveillance, de perquisition ou de saisie élargis par des lois récentes au Canada, au Royaume-Uni, en France et aux États-Unis », (2009) : http://www.priv.gc.ca/parl/2009/parl_bg_090507_f.pdf.

SYNTEC NUMÉRIQUE, « Livre blanc de la sécurité du Cloud Computing, Analyse des risques, réponses et bonnes pratiques », (2010) : http://www.syntec-numerique.fr/sites/default/files/related_docs/livre_blanc_cloud_computing_securite.vdef_.pdf.

THOMSON, Iain, « Snowden Leak : Microsoft added Outlook.com Backdoor for Feds », (2013) *The Register* : http://www.theregister.co.uk/2013/07/11/snowden_leak_shows_microsoft_added_outlookencryption_backdoor_for_feds/.

TREND MICRO, « Best Practices for Security and Compliance with Amazon Web Services », (2013) : http://deepsecurity.trendmicro.com/wp-system/uploads/2013/04/Trend-Micro-Best-Practices-for-Security-and-Compliance-with-Amazon-Web-Services.pdf.

U.S. ENVIRONMENTAL PROTECTION AGENCY, « Report to Congress on Server and Data Center Energy Efficiency Public Law 109-431 », (2007) : http://hightech.lbl.gov/documents/DATA_CENTERS/epa-datacenters.pdf.

U.S. GENERAL SERVICES ADMINISTRATION, « FedRAMP: Ensuring Secure Cloud Computing for the Federal Government » : http://www.gsa.gov/portal/category/102371?utm_source=OCSIT&utm_medium=print-radio&utm_term=fedramp&utm_campaign=shortcuts.

VAN HOBOKEN, Joris, Axel ANRBAK et Nico VAN EIJK, « Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act », (2012) *SSRN* : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534.

VAN OMMEREN, Erik, *et al.*, « Maîtrisez le cloud », (2011) IBM & Sogeti : http://www.fr.sogeti.com/sites/default/files/Documents/Publications/SOGETI_Maitrisez-leCloud.pdf.

VANDE GHINSTE, Bart, « Microsoft Cloud Continuum », (2010) : http://download.microsoft.com/download/7/3/C/73CACA9C-009D-46DC-88A2-5D92E1460A64/Hansver_I3_ISV_Cloud%20public.pptx.

WESTON, Greg, « Foreign Hackers Attack Canadian Government », (2013) *CBC.ca* : http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

WISPINSKI, Jennifer, « La « PatriotAct » des États-Unis et la *Loi Antiterroriste* du Canada : Principales différences entre les deux approches législatives », (2006) : http://www.parl.gc.ca/content/lop/researchpublications/prb0583-f.pdf.

ZETTER, Kim « Medical Records : Stored in the Cloud, Sold on the Open Market », (2009) : http://www.wired.com/threatlevel/2009/10/medicalrecords.

Autres documents

CENTRE DE SERVICES PARTAGÉS DU QUÉBEC, « Acquisition d'une solution SaaS pour le projet de dotation en ligne Sagir (SGR3) : Appel d'offres fondé sur le rapport qualité-prix ».

COMMISSION EUROPÉENNE, « Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis – Foire aux questions », MEMO/13/1059, 27 novembre 2013.

GOUVERNMENT DU QUÉBEC, « Guide relatif à la catégorisation des documents technologiques en matière de sécurité », Québec, 2003.

ONTARIO INFORMATION AND PRIVACY COMMISSIONER, « Privacy Investigation Report PC12-39 : Reviewing the Licensing Automation System of the Ministry of Natural Resources : A Special Investigation Report », (2012).

QUÉBEC, ASSEMBLÉE NATIONALE,

Journal des débats de la Commission permanente de la culture, 2e sess., 37e légis., 30 mai 2006, « Étude détaillée du projet de loi n° 86 – Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives », p. 1-45.

Journal des débats de la Commission permanente de la culture, 2e sess., 37e légis., 31 mai 2006, « Étude détaillée du projet de loi n° 86 – Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives », p. 11-32.

SERVICES GOUVERNEMENTAUX QUÉBEC, « Directive sur la sécurité de l'information gouvernementale », 2006, Québec.

TREMBLAY, Mathieu, « Services d'infonuagique (Synthèse de veille) », (2012) Laboratoire d'étude sur les politiques publiques et la mondialisation (LEPPM), École nationale d'administration publique.

TRUDEL, Pierre, « Analyse des enjeux et risques juridiques dans le cadre du projet pilote de « coffre-fort électronique » », (2012) à paraître.

Tables de la législation

Canada

Loi antiterroriste, L.C. 2001, c 41.

Loi constitutionnelle de 1867, 30 & 31 Victoria, c 3.

Loi sur l'accès à l'information, L.R.C. 1985, c A-1.

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5.

Loi sur la protection des renseignements personnels, L.R.C. 1985, c. P-21.

Loi sur le droit d'auteur, L.R.C. 1985, c. C-42.

Loi sur le service canadien du renseignement de sécurité, L.R.C. 1985, c. C-23.

Loi sur les télécommunications, L.C. 1993, c 38.

Québec

Charte des droits et libertés de la personne, RLRQ, c. C-12.

Code de procédure civile, RLRQ, c. C-25.

Code des professions, RLRQ, c. C-26.

Loi assurant l'exercice des droits des personnes handicapées en vue de leur intégration scolaire, professionnelle et sociale, RLRQ, c. E-20.1.

Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1.

Loi concernant le partage de certains renseignements de santé, RLRQ, c. P-9.0001.

Loi concernant les droits sur les mutations immobilières, RLRQ, c. D-15.1.

Loi facilitant le paiement des pensions alimentaires, RLRQ, c. P-2.2.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1.

Loi sur l'administration fiscale, L.R.Q., c A-6.002.

Loi sur l'Assemblée nationale, RLRQ, c. A-23.1.

Loi sur l'assurance maladie, RLRQ, c. A-29.

Loi sur l'impôt minier, RLRQ, c. I-0.4.

Loi sur l'Institut national de santé publique du Québec, RLRQ, c. I-13.1.1.

Loi sur l'acupuncture, RLRQ, c. A-5.1.

Loi sur l'aquaculture commerciale, RLRQ, c. A-20.2.

Loi sur la Caisse de dépôt et placement du Québec, RLRQ, c. C-2.

Loi sur la protection de la jeunesse, RLRQ, c. P-34.1.

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c. P-39.1.

Loi sur la protection du consommateur, RLRQ, c. P-40.1.

Loi sur la Régie du logement, RLRQ, c. R-8.1.

Loi sur la sécurité incendie, RLRQ, c. S-3.4.

Loi sur le Centre de services partagés du Québec, RLRQ, c. C-8.1.1.

Loi sur le curateur public, RLRQ, c. C-81.

Loi sur le notariat, RLRQ, c. N-3.

Loi sur le Régime des rentes du Québec, RLRQ, c. R-9.

Loi sur le Système correctionnel du Québec, RLRQ, c. S-40.1.

Loi sur les archives, RLRQ, c. A-21.1.

Loi sur les chemins de fer, RLRQ, c. C-14.1.

Loi sur les comptables agréés, RLRQ, c. C-48.

Loi sur les contrats des organismes publics, RLRQ, c. C-65.1.

Loi sur les normes du travail, RLRQ, c. N-1.1.

Loi sur les services de santé et les services sociaux pour les autochtones cris, RLRQ c S-5.

Loi sur les services de santé et les services sociaux, RLRQ c S-4.2.

Loi sur les services de santé et les services sociaux, RLRQ c S-4.2.

Loi sur les véhicules hors route, RLRQ c V-1.2.

Projet de loi n° 86 : *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, 2006, chapitre 22.

International

Anti-terrorism, Crime and Security Act 2001, 2001 c. 24.

Budget Transparency and Accountability Act, SBC 2000, c 23.

Foreign Intelligence Surveillance Act of 1978, 50 U.S. Code Chapter 36.

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

Loi de 2004 sur la Protection des renseignements personnels sur la santé, LO 2004, c 3, ann A.

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Loi sur l'accès et la protection en matière de renseignements personnels sur la santé, LN-B 2009, c. P-7.05.

Personal Health Information Act, SNL 2008, c. P-7.01.

Personal Information International Disclosure Protection Act, SNS 2006, c. 3.

Personal Information Protection Act, SA 2003, c. P-6.5.

Personal Information Protection Act, SBC 2003, c. 63.

Privacy Act 1988, n° 119, 1988 as amended.

Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

Public Safety Act, 2002, SC 2004, c. 15.

The Health Information Protection Act, SS 1999, c. H-0.021.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, PUBLIC LAW 107–56—OCT. 26, 2001.

Accords internationaux

Accord de commerce et de coopération entre le Québec et l'Ontario (ACCQO).

Accord de libéralisation des marchés publics du Québec et du Nouveau-Brunswick (AQNB 2008).

Accord entre le gouvernement du Canada et le gouvernement des États-Unis d'Amérique en matière de marchés publics (2010).

Accord intergouvernemental sur les marchés publics entre le gouvernement du Québec et le gouvernement de l'État de New York (AQNY).

Accord sur les marchés publics (AMP) de l'Organisation mondiale du commerce.

Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886, complétée à PARIS le 4 mai 1896, révisée à BERLIN le 13 novembre 1908, complétée à BERNE le 20 mars 1914 et révisée à ROME le 2 juin 1928, à BRUXELLES le 26 juin 1948, à STOCKHOLM le 14 juillet 1967 et à PARIS le 24 juillet 1971 et modifiée le 28 septembre 1979.

Table de la jurisprudence

Décisions canadiennes

Air Atonabee Ltd. (f.a.s. City Express) c. *Canada (Ministre des Transports)*, [1989] A.C.F. n° 453.

Apple Computer, Inc. c. *Mackintosh Computers Ltd.*, (1987) 18 C.P.R. (3d) 129.

Astrazeneca Canada Inc. c. *Canada (Ministre de la Santé)*, 2005 CF 189.

B.C.G.E.U. v. *British Columbia (Minister of Health Services),* 2007 BCCA 379.

Bourque c. *Zangwill*, 2002 CanLII 9546 (QC CQ).

Cadbury Schweppes Inc. c. *Aliments FBI Ltée*, [1999] 1 RCS 142.

Canadian Admiral Corp. c. *Rediffusion Inc.*, [1954] 20 C.P.R. 75.

CCH Canadienne Ltée c. *Barreau du Haut-Canada*, 2002 CAF 187.

CCH Canadienne Ltée c. *Barreau du Haut-Canada*, 2004 CSC 13.

CPVPC, « Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA Patriot Act* », Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2005-313.

Delisle c. *Shawinigan Water & Power Co.*, [1968] R.C.S. 744.

eBay Canada Ltd. c. *M.R.N.*, 2008 CAF 348.

GIFRIC inc. c. *Corporation Sun Média (Journal de Québec)*, 2009 QCCA 236.

Gordon c. *Canada (Santé)*, 2008 CF 258.

Gyulai c. *Montréal (Ville de)*, 2009 QCCQ 1809.

Institut de zoothérapie du Québec Inc. c. *Rioux*, 2005 CanLII 10507 (QC C.S.).

Lac minerals ltd. c. *International corona resources ltd.*, [1989] 2 RCS 574.

Lehman c. *Pratt & Whitney Canada Corporation*, 2007 QCCS 3888.

M.R. c. *Centre des services partagés du Québec*, 2010 QCCAI 3000.

Merck Frosst Canada Ltée c. *Canada (Santé)*, 2012 CSC 3.

Montréal (Ville de) c. *Cour du Québec*, 2009 QCCS 2895.

Montréal (Ville de) c. *Gyulai*, 2011 QCCA 238.

Municipalité de Val-des-Monts c. *Québec (Ministère du Développement durable, de l'Environnement et des Parcs*), 2009 QCCAI 177.

Office du crédit agricole du Québec c. *Boucher*, (c.p.) [1987] C.A.I., 252, 254.

Pharand Ski Corp. v. *Alberta*, 1991 CarswellAlta 85 (ABQB).

Public Service Commission (Re), 2013 CanLII 55439 (SK IPC).

R. c. *Multiform Manufacturing Co.*, [1990] 2 R.C.S. 624.

R. c. *Stewart*, [1988] 1 R.C.S. 963, par. 33.

R.L. Crain Limited v. *R.W. Ashton & Ashton Press Mfg. Co. Ltd.*, [1949] 2 D.L.R. 481.

R.L. Crain Limited v. *R.W. Ashton & Ashton Press Mfg. Co. Ltd.*, [1950] 1 D.L.R. 601.

Richard c. *Gougoux*, 2009 QCCS 2301.

Saltman Engineering Co. v. Campbell Engineering Co. (1948), 65 R.P.C. 203 (C.A.).

Sécurité des Deux-Rives ltée c. *Groupe Meridian construction restauration inc.*, 2013 QCCQ 1301.

Société Gamma Inc. c. *Canada (Secrétariat d'État)*, [1994] A.C.F. n^{o} 589.

Théberge c. *Galerie d'Art du Petit Champlain inc.*, 2002 CSC 34.

Décisions étrangères

Ansell Rubber Co. c. *Allied Rubber Industries Pty. Ltd.*, [1967] V.R. 37.

Décision n° 2000/520/CE du 26 Juillet 2000.

Décision n° 2002/2/CE du 20 décembre 2001.

Deta Nominees Pty. Ltd. c. *Viscount Plastics Products Pty. Ltd.*, [1979] V.R. 167.

ANNEXE 1 – Lexique

Sauf indications contraires, toutes les définitions contenues dans la présente annexe émanent du site *granddictionnaire.com* de l'Office de la langue française.

Administrateur système - « Personne chargée de la configuration d'un système multiutilisateur fonctionnant à l'intérieur d'un réseau, et de la gestion du va-et-vient des utilisateurs de ce système. C'est notamment à l'administrateur de système qu'incombent les tâches suivantes : l'attribution ou l'annulation des mots de passe, l'installation des interfaces utilisateurs, l'installation ou la suppression des logiciels d'application et la sauvegarde des données ».

ASP (Application Service Provider – ou fournisseur d'applications hébergées**)** – « Société qui offre en location, souvent en ligne, des progiciels ou des logiciels d'application avec tous les services connexes ».

Architecture de réseau - « L'architecture d'un réseau décrit principalement les équipements de connexion, les ressources logicielles, les méthodes d'accès, les protocoles et les liaisons qu'il utilise pour la transmission des données. »

Application - « Ensemble de programmes informatiques qui servent à aider un utilisateur à faire un certain travail. »

Applications à la demande - « Modèle de distribution en ligne de logiciels dans lequel un usager obtient la copie de l'un d'entre eux d'un hébergeur à qui il doit payer une somme d'argent pour son usage. »

Authentification - « Procédure consistant à vérifier ou à valider l'identité d'une personne ou l'identification de toute autre entité, lors d'un échange électronique, pour contrôler l'accès à un réseau, à un système informatique ou à un logiciel. »

Bande passante - « Capacité d'une voie de communication à transmettre des données. »

Base de données - « Ensemble structuré d'éléments d'information, généralement agencés sous forme de tables, dans lesquelles les données sont organisées selon certains critères en vue de permettre leur exploitation. »

Bureau virtuel - « Environnement informatique qui permet à un groupe de personnes, généralement éloignées les unes des autres, de travailler ensemble à partir d'appareils qui leur permettent de communiquer à distance. »

Business Process as a Service (BPaaS) - « Livraison de services d'impartitions de processus d'affaires qui proviennent du nuage et sont construits pour l'architecture partagée. Les services sont souvent automatisés et, lorsqu'une intervention humaine est nécessaire, il n'y a pas de bassin d'emploi ouvertement dédié à chaque client. Les modèles de tarification sont basées sur la consommation ou fonctionne par abonnementé »[651]

Centre de données - « Lieu, organisme ou unité administrative où sont regroupées les opérations relatives au traitement de l'information, notamment à des fins de gestion, pour une entreprise ou un groupe de personnes. »

Charges de travail - « Ensemble des tâches devant être effectuées par une ou des ressources, ou un ou des éléments de configuration. Les charges de travail représentent généralement des applications spécifiques qui peuvent être subdivisées par type de travail, par exemple : interactif, à temps partagé, par lot. La charge de travail, qui est déterminée par des techniques de modélisation de la gestion de la capacité, sert à faire des prévisions d'utilisation des ressources. »

Chiffrement - « Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale, » ou « [o]pération par laquelle on transforme des données confidentielles au moyen d'une clé privée (**clé de chiffrement**), pour les rendre inintelligibles aux personnes ne possédant pas cette clé, et en empêcher l'accès ou l'altération sans autorisation au cours d'un traitement ou d'une transmission par ligne de communication. »

Communication - « Transmission d'informations effectuée entre des équipements informatiques, conformément à des conventions préétablies. La transmission des informations peut s'effectuer entre plusieurs ordinateurs ou périphériques, et même entre logiciels. Elle se fait donc par modem, par réseaux, par bus ou interface logicielle. »

Confidentialité - « Propriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées »

Configuration - « Combinaison des composants matériels ou logiciels, déterminant les caractéristiques essentielles de fonctionnement. Le choix de la vitesse du microprocesseur, de la capacité de la mémoire, du disque dur, du système d'exploitation, des périphériques, des connexions et des unités fonctionnelles fait partie de la configuration matérielle d'un système informatique. Le type de représentation des données, le nombre, la position et la taille des objets, la définition de l'animation des objets, l'alignement des objets, l'affichage des boîtes de dialogue (fenêtres) représentent la configuration logicielle. La configuration sera définie en fonction des applications et des utilisations qui sont envisagées. Bien que la configuration d'un système puisse être modifiée (ajout de mémoire vive ou augmentation de la capacité du disque dur, etc.), l'architecture d'un système reste, en général, inchangée. »

[651] GARTNER, « IT Glossary » : http://www.gartner.com/it-glossary/business-process-as-a-service-bpaas/.

Correctif - « Fichier contenant une liste de modifications à apporter à un programme dans le but d'ajouter des fonctionnalités, de corriger un bogue ou un dysfonctionnement ou de faire une mise à jour. »

Corruption de données – « Perte ou dégradation, volontaire ou accidentelle, de données conservées sur un support informatique. »

Coupe-feu (ou pare-feu) - « Dispositif informatique qui permet le passage sélectif des flux d'information entre deux réseaux, ainsi que la neutralisation des tentatives de pénétration extérieures ».

Courriel - « Message transmis par un utilisateur vers un ou plusieurs destinataires, d'ordinateur à ordinateur, par l'intermédiaire d'un réseau informatique, favorisant entre eux un échange rapide et sans frontières. »

Cryptage - Voir « chiffrement »

Cryptographie - « Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité. »

Cryptographie à clé publique - « Cryptographie dans laquelle on utilise une paire de clés asymétriques, une clé publique et la clé privée correspondante, pour chiffrer et déchiffrer les données. »

Cyberattaque - « Attaque informatique qui vise à endommager ou à détruire des réseaux ou des systèmes informatiques. »

Cybersécurité - « Protection des systèmes informatiques, des programmes et des données traitées, mémorisées et transmises par les systèmes contre les accidents et les actes malveillants au moyen de politiques et procédures de contrôle appropriées. »

Cycle de vie - « Ensemble des étapes que franchit un document (électronique ou non) et qui vont de sa conception à sa destruction, en passant par sa diffusion et son archivage. »

Data as a Service - « Data as a Service (DaaS) est un modèle de provision et de distribution de l'information selon lequel des fichiers (incluant des fichiers textes, images, sonores et vidéos) sont mis à la disposition de clients par le biais d'un réseau, normalement l'Internet. »[652]

Déploiement - « Ensemble des activités qui consistent à livrer, installer et mettre en service un ensemble intégré d'éléments de configuration, nouveaux ou modifiés, dans l'infrastructure technologique d'une organisation. »

---

[652] Margaret ROUSE, « Data as a service », (2012) *Search Cloud Applications*, en ligne : < http://searchcloudapplications.techtarget.com/definition/data-as-a-service >.

Desktop as a Service (DTaaS) - **«** Le DTaaS, ou bureau en tant que service, est l'externalisation du poste de travail auprès d'un prestataire de services. »

Diligence raisonnable - « Degré de prudence, d'activité, de réaction et d'attention auquel on peut à bon droit s'attendre de la part d'une personne raisonnable et prudente et dont fait habituellement preuve cette personne raisonnable et prudente face à une situation donnée. »

Disponibilité - « Propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite. »

Document technologique - « Document constitué d'informations délimitées et structurées de façon logique et portées par un support faisant appel aux technologies de l'information »[653].

Domain Name System - « Système distribué de bases de données et de serveurs, qui assure la traduction des noms de domaine utilisés par les internautes en numéros Internet utilisables par les ordinateurs, ceci pour permettre la transmission des messages d'un site à l'autre du réseau. »

Données personnelles - Voir « Renseignement personnel »

Droit d'auteur - « Droit exclusif que détient un auteur ou son mandataire d'exploiter à son profit, pendant une durée déterminée, une œuvre littéraire, artistique ou musicale. »

Équipement informatique - « Ensemble du matériel et des logiciels nécessaires pour mener à bien une activité informatique. »

Espace disque - « Espace disponible sur un disque, servant à l'écriture de données supplémentaires. »

Fiabilité – « Propriété d'un système informatique capable d'assurer ses fonctions sans défaillance, dans des conditions préalablement définies et sur une période déterminée. »

Fournisseur de services infonuagiques - « Entreprise qui héberge et met à la disposition des organisations et des particuliers, répartis localement ou partout dans le monde, des infrastructures-services, des plateformes-services et des logiciels-services sur Internet, qui les gère et qui en assure la maintenance. »

Fragmentation - « Situation où une mémoire de masse présente beaucoup de vides séparés et nécessite un compactage. »

Gestion des identités - « Activité de gestion qui commande l'authentification et l'habilitation des utilisateurs afin de contrôler leur accès à des ressources informatiques ou à des technologies de l'information. »

---

[653] *LCCJTI*, art. 3.

Hardware - « Ensemble des éléments physiques d'une installation informatique. »

Héberger – « Fournir un certain espace mémoire à un site Web sur un serveur et le diffuser dans Internet. »

Hébergement - « Action d'héberger un site Web ou une page personnelle sur un serveur, afin de les rendre accessibles sur Internet. »

Impartition - « Prise en charge contractuelle, par un prestataire extérieur, de la totalité ou d'une partie des ressources informatiques d'une entreprise. »

Infonuagique - « Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. »

Information confidentielle - « Information sur une entreprise, un produit, un service, protégée ou non par le droit d'auteur ou par un brevet, information nominative sur des individus, qui est traitée électroniquement et accessible par l'intermédiaire d'un réseau, dont la divulgation accidentelle ou voulue pourrait porter préjudice à l'une des parties en cause, et que l'on protège par des moyens techniques (par un coupe-feu, par exemple) ou en restreignant son accès à certaines personnes autorisées. »

Informatique - « Discipline qui s'intéresse à tous les aspects, tant théoriques que pratiques, reliés au traitement automatique de l'information, à la conception, à la programmation, au fonctionnement et à l'utilisation des ordinateurs. »

Infrastructure - « Ensemble des éléments de configuration utilisés dans la prestation des services des TI, qui comprend le matériel informatique, les logiciels, les installations, les ressources humaines, la documentation et les données. »

Infrastructure as a Service - « Infrastructure prête à l'emploi, louée à la demande chez un fournisseur de services, accessible par Internet ou par le réseau d'une organisation, ou par les deux à la fois. »

Installation - « Opérations nécessaires pour rendre un matériel ou un logiciel apte à fonctionner sur un équipement spécifique. »

Intégrité - « Propriété associée aux données qui, lors de leur traitement ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. »

Interface de programmation - « Ensemble de routines standards, accessibles et documentées, qui sont destinées à faciliter au programmeur le développement d'applications. »

Intrusion - « Opération qui consiste à accéder, sans autorisation, à un système informatique ou à un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place. »

Langage de programmation - « Langage artificiel comprenant un ensemble de caractères, de symboles et de mots régis par des règles qui permettent de les assembler, utilisé pour donner des instructions à un ordinateur. »

Licence - « Autorisation conférant le droit, exclusif ou non exclusif, d'exploiter un titre de propriété industrielle sans en devenir pour autant propriétaire. »

Lignes de code - « Ligne de programme source qui contient habituellement une instruction en langage de programmation. »

Logiciel - « Ensemble de programmes permettant d'effectuer un traitement particulier sur un ordinateur. »

Logiciel hérité - Voir « système hérité ».

Logiciel malveillant - « Logiciel destiné à endommager tout ou partie des éléments nécessaires au fonctionnement d'un système informatique. »[654]

Logiciel de gestion de systèmes - « Logiciel développé par la firme Microsoft, conçu pour simplifier la gestion des ordinateurs reliés en réseau dans l'entreprise, en automatisant les tâches d'inventaire, de distribution logicielle et de contrôle à distance. »

Métadonnées - « Informations sur les données météorologiques et climatiques, indiquant à quel moment et de quelle manière elles ont été mesurées, leur degré de qualité, les problèmes rencontrés et d'autres caractéristiques. »

Modèle de déploiement - « La notion de modèle de déploiement fait référence à la manière selon laquelle est mis en œuvre un nouveau système informatique. »

Modèle de service - « La notion de modèles de service renvoie aux types de ressources auxquelles un utilisateur du nuage peut avoir accès. »

Module logiciel - « Unité matérielle fonctionnelle destinée à être utilisée en conjonction avec d'autres composants. »

Navigateur - « Logiciel qui permet de consulter sur Internet les pages Web et de circuler dans les différents moteurs de recherche. »

Network as a Service (NaaS) - **«** Les prestataires de services NaaS fournissent un réseau privé virtuel avec bande passante sur demande à leurs clients. Ces derniers n'ont donc pas à investir

[654] DICTIONNAIRE REVERSO, « logiciel malveillant », en ligne : < http://dictionnaire.reverso.net/francais-definition/logiciel%20malveillant >.

dans un réseau local, mais peuvent simplement utilisé le réseau fourni selon une formule de paiement selon l'utilisation, ou mensuelle. »[655]

Outil de programmation - « Programme utilisé pour aider au développement des programmes et à la maintenance des systèmes. »

Output - « Processus qui permet à un système d'exploitation ou à un programme d'application de transférer des données vers un périphérique de sortie tel que l'écran ou l'imprimante, ou de les stocker sur disque ou dans un fichier, ou encore de les envoyer vers un autre ordinateur par un réseau. »

Packets - Voir « paquets de données ».

Paquets de données - « Ensemble de bits et d'éléments numériques de service constituant un message ou une partie de message, organisé selon une disposition déterminée par le procédé de transmission et acheminé comme un tout. »

Programmation - « Ensemble des activités techniques reliées à l'élaboration d'un programme informatique. La programmation comprend des activités de conception, d'écriture, de test et de maintenance de programmes pour ordinateurs. »

Pare-feu - Voir « coupe-feu ».

Périmètre de sécurité - « Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais sa définition doit aussi englober (ou pas) les entités immatérielles qui peuplent les ordinateurs et les réseaux, essentiellement les logiciels et en particulier les systèmes d'exploitation. »[656]

Pirate - « Personne qui contourne ou détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique. »

Platform as a Service - « Plateforme prête à l'emploi, louée à la demande chez un fournisseur de services, accessible par Internet ou par le réseau d'une organisation, ou par les deux à la fois. La plateforme-service est accessible par Internet dans le cas d'un nuage public, par le réseau d'une organisation dans celui d'un nuage privé ou par les deux à la fois dans le cas d'un nuage hybride. La plateforme-service met à la disposition des développeurs un environnement d'exécution (système d'exploitation, matériel, réseau) qui leur permet d'installer ou de créer leurs propres logiciels. »

---

[655] Margaret ROUSE, « Network-as-a-service », (2013) *Search SDN*, en ligne : < http://searchsdn.techtarget.com/definition/Network-as-a-Service-NaaS >.

[656] Laurent BLOCH et Christophe WOLFHUGEL, Sécurité informatique – Principes et méthodes, 3e éd., Paris, Eyrolles, 2011, p. 10.

Plateforme - « Structure matérielle d'un système informatique, principalement basée sur le type de système d'exploitation utilisé. »

Prestataire de services d'hébergement - « Fournisseur proposant un service d'hébergement, gratuit ou payant, qui permet de disposer d'un espace disque sur son serveur, afin de diffuser sur Internet des sites Web ou des pages personnelles. »

Prestataire de services infonuagiques - Voir « fournisseur de service infonuagiques »

Propriété intellectuelle - « Droit de propriété sur une création de l'esprit, par exemple une œuvre littéraire, une découverte scientifique, une prestation artistique. »

Protocole Internet - « Protocole de la suite TCP-IP qui régit la circulation des informations à travers des réseaux hétérogènes, en fragmentant, à la source, ces informations sous forme de paquets de données contenant notamment l'adresse du destinataire, puis en les rassemblant à l'arrivée. »

Renseignements confidentiels - « Tout renseignement dont la loi ou une convention entre les parties (sous réserve de ce qui est autorisé par la loi) en interdit la divulgation volontaire ou involontaire à un tiers (à l'exception, dans certains cas, de la personne concernée). »

Renseignements personnels - « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier »[657]. « Les renseignements personnels sont confidentiels »[658].

Réseau - « Ensemble d'équipements qui sont reliés les uns aux autres par des câbles ou des faisceaux hertziens, afin qu'ils puissent échanger, distribuer ou diffuser des informations et partager différentes ressources. »

Réseautage social - « Utilisation des réseaux sociaux à des fins d'interaction entre individus ou organisations. »

Secret industriel - « Connaissances tenues secrètes ayant une valeur industrielle, notamment pour ce qui est des renseignements utilisés dans la fabrication; ces connaissances ne peuvent, ou peuvent difficilement, s'acquérir par l'examen du produit ou procédé industriel et ne sont connues que d'un nombre limité de personnes qui sont tenues de ne pas les communiquer. »

Sécurité - « Protection des systèmes informatiques, des programmes et des données traitées, mémorisées et transmises par les systèmes contre les accidents et les actes malveillants au moyen de politiques et procédures de contrôle appropriées. »

---

[657] *Loi sur la protection des renseignements personnels dans le secteur privé*, art. 2.

[658] *Loi sur l'accès*, art. 54.

Sécurité de l'information - « Protection des ressources informationnelles d'une organisation, face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée. »

Sécurité informatique - « Ensemble de mesures de sécurité physiques, logiques et administratives, et de mesures d'urgence, mises en place dans une organisation, en vue d'assurer la protection de ses biens informatiques, la confidentialité des données de son système d'information et la continuité de service. »

Sécurité informationnelle - « Protection des ressources informationnelles d'une organisation, face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée. »

Serveur - « Dans un réseau, ordinateur qui exécute le logiciel d'administration et qui contrôle l'accès au réseau et à ses ressources (par exemple les disques durs et les imprimantes), et leur partage. Un serveur peut héberger notamment des bases de données consultables à partir des postes de travail reliés au réseau. »

Service de courriel - « Service de correspondance qui permet l'échange de messages électroniques à travers un réseau informatique. »

Sites de réseautage social - « Sites Web utilisées à des fins d'interaction entre individus ou organisations. »

Site Web malicieux - « Site Web infecté de logiciels malveillants ou transmettant de tels logiciels à ses visiteurs. »

Software as a Service - « Logiciel prêt à l'emploi, loué à la demande chez un fournisseur de services, accessible par Internet ou par le réseau d'une organisation, ou par les deux à la fois. Le logiciel-service est accessible par Internet dans le cas d'un nuage public, par le réseau d'une organisation dans celui d'un nuage privé ou par les deux à la fois dans le cas d'un nuage hybride. »

Storage as a service - « Le Staas, ou stockage à la demande, consiste en la location d'espace serveur, notamment afin d'héberger des copies de sauvegarde. Ce modèle de service fonctionne normalement selon un modèle d'affaire de paiement par gigaoctet utilisé. »

Support matériel - « Tout support permettant de transporter des données (clé USB, disque dur externe, etc.). »

Système informatique - « Ensemble des éléments matériels (l'ordinateur et ses périphériques) et logiciels nécessaires au traitement des données. »

Système opérationnel - ««Ensemble des activités, de l'équipement, des installations et de l'outillage nécessaires à la production d'un bien ou d'un service. »

Temps de latence - « Quantité de temps qu'on doit compter pour qu'un signal effectue le trajet d'un point à un autre dans un réseau de télécommunication. »

Traitement - « Exécution des instructions d'un programme par l'unité centrale, qui se traduit en une série d'opérations logiques ou d'opérations de calcul effectuées sur des données ou des informations, entre le moment où celles-ci sont entrées dans un système informatique et celui où elles en sortent. »

Tiers-fournisseur de service - « Personne ou entité qu'une entreprise a engagée par contrat en recourant à l'externalisation, afin que cette personne ou entité lui fournisse certains services ou exécute à sa place certaines activités. »

Transmission - « Envoi de données ou d'un signal, d'un point à un autre, en utilisant un ensemble de moyens spécialisés telle une ligne de communication. »

Transparence - « Qualité d'une organisation qui informe sur son fonctionnement, ses pratiques, ses intentions, ses objectifs et ses résultats. »

Virtualisation - « Ensemble des techniques logicielles ou matérielles qui permettent de regrouper sur un seul support physique des ressources informatiques, afin qu'elles puissent effectuer séparément des tâches spécifiques, comme si elles étaient exécutées sur des supports physiques distincts. La virtualisation permet de suppléer au manque de ressources de certains supports informatiques (disque dur, mémoire, unité de stockage, serveur, système d'exploitation, réseau, etc.). »

Vulnérabilité - « Faiblesse d'un système se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent. »

Workplace as a service - Environnement de travail virtuel permettant l'utilisation de divers appareils (ordinateurs, tablettes, téléphones intelligents, etc.) [659]. En fait, la principale caractéristique du Wpaas est que ce modèle de service mise sur le concept du « prenez vos appareils personnels », une « [p]ratique consistant, pour un employé, à utiliser son matériel électronique personnel dans le cadre de son travail ».

[659] Voir : < http://www.econocom.com/fr/nos-metiers/services-it/workplace-as-a-service >.

ANNEXE 2 – Liste de contrôles