Université de Montréal

# Le cadre juridique applicable à une infrastructure sous forme de service (IaaS) dans le milieu universitaire

par
Jean-Sébastien Décarie

Centre de recherche en droit public
Faculté de droit

Mémoire présenté à la Faculté de droit
en vue de l'obtention du grade de Maîtrise
en droit des technologies de l'information (LL.M.)

Mai 2019

# Résumé

L’infonuagique est une notion très vaste qui couvre une multitude de services en lignes que nous utilisons tous, sans nécessairement en avoir connaissance. Elle est subdivisée en différents modèles de prestation de service, l'un d'eux est l'infrastructure sous forme de service. Ce modèle est défini comme étant une infrastructure prête 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. Cette technologie en essor est convoitée dans tous les domaines, notamment par le milieu universitaire. Évidemment, l'utilisation d'une telle technologie soulève de nombreuses questions juridiques en matière de sécurité de l'information et de l'obligation d’assurer la confidentialité, l'intégrité, et la disponibilité des données portée vers ces systèmes. L'objectif du présent mémoire est donc de définir le cadre législatif applicable à l'infrastructure sous forme de service en milieu universitaire afin de mieux préparer les établissements à la migration vers cet environnement.

**Mots-clés** : Infonuagique, Infrastructure sous forme de service, IaaS, Obligation de sécurité, Confidentialité, Intégrité, Disponibilité, sécurité informationnelle, nouvelles technologies.

# Abstract

Cloud Computing is a very broad concept that covers a multitude of online services that we all use, without necessarily being aware of it. It is subdivided into different service delivery models, one of which is the infrastructure as a service which is defined as a ready-to-use infrastructure, leased on demand from a service provider, accessible through the Internet or by the network of an organization, or both. This constantly evolving technology is coveted in all areas, especially by the academic community. Of course, the use of such technology raises many legal issues regarding information security and the obligation to ensure confidentiality, integrity, and availability of data found on these systems. The objective of this master's thesis is therefore to define the legislative framework applicable to the infrastructure as a service model in order to better prepare institutions wishing to migration to this environment.

**Keywords** : Cloud computing, infrastructure as a service, IaaS, infrastructure, security obligation, confidentiality, integrity, availability, informational security, information technology.

# Table des matières

# Liste des tableaux

# Liste des figures

# Liste des sigles

| | |
|---|---|
| API | *Application Programming Interface* |
| CaaS | *Communication as a Service* |
| C.c.Q. | Code civil du Québec |
| C.A.I. | Commission d'accès à l'information du Québec |
| CEI | Commission Électrotechnique Internationale |
| CID | Confidentialité, Intégrité, Disponibilité |
| CRDI | Centre de recherches pour le développement international |
| CRSH | Conseil de recherches en sciences humaines |
| CRSNG | Conseil de recherches en sciences naturelles et en génie du Canada |
| CSA | *Cloud Security Alliance* |
| CSP | *Cloud Service Provider* |
| CSPQ | Centre de services partagés du Québec |
| CPVPC | Commission d'accès à l'information du Québec |
| DaaS | *Desktop as a Service* |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | *Domain Name System* |
| DDoS | *Distributed Denial of Service* |
| EULA | *End User License Agreement* |
| FCI | Fondation canadienne pour l'innovation |
| FRQ-NT | Fonds de Recherche du Québec - Nature et les technologies |
| FRQ-SC | Fonds de Recherche du Québec - Société et Culture |
| FRQ-S | Fonds de recherche du Québec – Santé |
| GCP | *Google Cloud Platform* |
| IaaS | *Infrastructure as a Service* |
| IEC | *International Electrotechnical Commission* |
| IEEE | *Institute of Electrical and Electronics Engineers* |
| ISO | *International Organization for Standardization* |
| IT | *Information Technology* |
| IRSC | Institut de Recherche en Santé du Canada |

| | |
|---|---|
| LDAP | *Lightweight Directory Access Protocol* |
| LPRPSP | Loi sur la protection des renseignements personnels dans le secteur privé |
| LCCJTI | Loi concernant le cadre juridique des technologies de l'information |
| LPRPDÉ | Loi sur la protection des renseignements personnels et des documents Électroniques |
| MaaS | *Monitoring as a Service* |
| MDEIE | Ministère de l'Économie, de l'Innovation et des Exportations Québec |
| NAS | Numéro d'Assurance Sociale |
| NDA | *Non-Disclosure Agreement* |
| NIST | *National Institute of Standards and Technology* |
| OQLF | Office Québécois de la langue française |
| OSBL | Organisme sans but Lucratif |
| PaaS | *Platform as a Service* |
| PBX | *Private branch exchange* |
| PCI | *Payment Card Industry* |
| PII | *Personally Identifiable Information* |
| RISQ | Réseau d'informations scientifiques du Québec |
| SaaS | *Software as a Service* |
| SCT | Secrétariat du Conseil du Trésor |
| SLA | *Service Level Agreement* |
| SPI | *Software, Platform, Infrastructure* |
| SSL | *Secure Sockets Layer* |
| TCP/IP | *Transmission Control Protocol / Internet Protocol* |
| TI | Technologie de l'Information |
| TLS | *Transport Layer Security* |
| UIT | Union internationale des télécommunications |
| VDI | *Virtual Desktop Infrastructure* |
| VM | *Virtual Machine* |
| VoIP | *Voice Over Internet Protocol* |
| VPN | *Virtual Private Network* |
| XaaS | Anything as a Service |

# Remerciements

À la fin d’un cours de deuxième cycle, dans le cadre de mon microprogramme en droit des TI, Le professeur Nicolas W. Vermeys m’a dit : « Pourquoi ne pas faire une maîtrise ? Après tout c’est seulement 4 travaux comme vous venez de faire ! ». Ce n’était pas tout à fait exact, une maîtrise est loin d'être un travail si simple. Néanmoins, à la conclusion de cette rédaction, je ne peux que lui être reconnaissant de m’avoir incité à accomplir cette lourde tâche, et surtout pour m’avoir inculqué cet intérêt toujours grandissant envers le droit des technologies de l’information.

Merci à mes amis qui m’ont épaulé pendant cette longue conquête que fût la recherche, l’étude et la rédaction de mon mémoire. Benoit, Sébastien, Victor et tous les autres, vous êtes très important pour moi. Merci à mes collègues et patrons qui ont accepté toutes ces journées de « congé »! Merci également à mes parents pour leurs encouragements à persévérer dans mes études, et à ma sœur Geneviève pour ses corrections !

Un merci tout spécial à ma conjointe Janik, qui m’a appuyé dans cette démarche et qui a enduré ces longs moments de rédaction. Merci, Zoé et Olivier, un jour vous comprendrez pourquoi papa passait de si longues heures à la rédaction de son mémoire.

# Introduction

En tant que pilier important de l'économie du savoir, les universités ont, sans l'ombre d'un doute, toujours influencé les technologies informationnelles, et ce, depuis l'avènement de l'Internet, qui a justement débuté en partie entre leurs murs[1]. Le milieu universitaire œuvre continuellement afin d'offrir aux étudiants et étudiantes des services à la fine pointe des technologies. Les universités québécoises, souvent contraintes financièrement par des diminutions ou des restrictions budgétaires[2], se doivent d'innover continuellement et d'offrir à leurs clientèles étudiantes un environnement d'apprentissage ainsi que de recherche moderne et efficace.

Au cours des dernières années, les données informatiques se sont plus que quintuplées. La majeure partie de l'information actuellement traitée dans les universités québécoises repose sur la forme d'octets. Également, les organisations et les entreprises privées utilisant les technologies de l'information ont entamé, au cours des dernières années, une métamorphose avec l'avènement de nouvelles solutions infonuagiques. La formation universitaire, considérée comme la clé du succès dans une société et une économie moderne, se doit de suivre ces changements.

Il suffit de prendre connaissance de l'objet instauré par le 1er article de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*[3] pour comprendre la tendance du gouvernement en ce qui a trait à la gestion des ressources informationnelles.

> « 1. La présente loi a pour objet d'établir des règles de gouvernance et de gestion en matière de ressources informationnelles applicables aux publics et aux entreprises du gouvernement afin notamment:
>
> 1° d'instaurer une gouvernance intégrée et concertée, fondée sur la préoccupation d'assurer des services de qualité aux citoyens et aux entreprises de même que la pérennité du patrimoine numérique gouvernemental;

---

[1] Pierre TRUDEL *et al*., *Droit du cyberespace*, Montréal, Thémis, 1997, p. 1-32.
[2] G. GIRARD, C. GRONDIN, *Le financement des universités, Historique, explications et recommandations pour une nouvelle formule de financement*, Union Étudiante du Québec, 2017 page 68.
[3] *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, L.R.Q., c. G-1.03.

> 2° d'optimiser les façons de faire en privilégiant le partage et la mise en commun du savoir-faire, de l'information, des infrastructures et des ressources;
>
> 3° d'assurer une planification rigoureuse et transparente de l'utilisation des sommes consacrées aux ressources informationnelles favorisant notamment une gestion efficiente des fonds publics;
>
> 4° de favoriser les meilleures pratiques en matière de gestion de projets en ressources informationnelles;
>
> 5° de permettre la mise en œuvre d'orientations communes à l'ensemble des organismes publics. »[4] (nos soulignements).

Qui plus est, le ministre délégué à la transformation numérique gouvernementale, Éric Caire a aussi annoncé au début février 2019 que « l'État veut transférer 80 % de ses données à des services d'hébergement en ligne privés, comme ceux d'Amazon, de Google ou encore de Microsoft. »[5]. Interrogé sur la protection des données personnelles, le ministre a rappelé que « Amazon détient des serveurs au Québec, notamment à Varennes. »[6].

En dépit de la protection de nos données, le passage vers l'informatique « dans les nuages »[7] est souvent perçu comme une panacée. Cette tendance mondiale en matière d'acquisition de services technologiques offre comme objectifs de diminuer les frais d'exploitation des infrastructures informatiques et des applications.

Dans cette économie menée par la connaissance, l'information constitue un des atouts les plus importants d'une université. Alors pourquoi donc voudrions-nous nous confier la garde à un tiers ? Notamment pour des raisons technologiques, économiques ou politiques.

Débutons avec les raisons technologiques. Depuis maintenant plusieurs décennies, les ordinateurs ont fait leur apparition. Bien avant de tenir dans le creux de nos mains, ils ont démarré comme une technologie hautement centralisée. Les premiers ordinateurs centraux comme le 700 d'IBM pesaient jusqu'à 16 tonnes et comprenaient 1 700 tubes à vide[8]. À cette

---

[4] *Id*., p. 1.
[5] Delphine JUNG, « Québec confiera le stockage des données publiques au privé », (Février 2019*), ICI Radio-Canada*, en ligne : <https://ici.radio-canada.ca/nouvelle/1150932/centres-donnees-informatiques-cti-ibm-amazon-caire> (consulté le 28 avril 2019).
[6] *Id*.
[7] Le nuage fait souvent référence au côté abstrait et de l'ubiquité des données.
[8] Dan SULLIVAN, « a brief history of decentralized computing », (Août 2018) Samsung NEXT, en ligne : <https://samsungnext.com/whats-next/a-brief-history-of-decentralized-computing/> (consulté le 28 avril 2019).

époque, le prix du matériel de même que celui de la main-d'œuvre spécialisée requise afin de programmer et d'utiliser ces imposantes machines ont favorisé cette centralisation. L'introduction des ordinateurs personnels, dans les années 1980, a amorcé le premier changement majeur de l'informatique et a inévitablement mené à la décentralisation de ces derniers[9]. Le traitement de l'information fut déplacé des ordinateurs centraux vers les ordinateurs de bureaux. Un second cycle de centralisation s'est produit au milieu des années 80. Ce changement de paradigme fut causé en partie par la création des bases de données relationnelles, mais également par le manque de normes de réseautage permettant aux ordinateurs de communiquer facilement entre eux. Par la suite, au début des années 90, les architectures clients/serveur ont fait leur apparition. L'avènement des liens Ethernet[10] et des connexions « *token ring* »[11] a permis de normaliser les réseaux informatiques que l'on connaît aujourd'hui. Cette période a notamment été enrichie par l'amélioration des performances des systèmes de bureautique ainsi que par l'avènement d'interfaces plus conviviales pour les utilisateurs. C'est aussi à cette époque que l'arrivée des jeux vidéo a incité les familles à se procurer un ordinateur[12] sur lequel nous nous sommes hâtés d'entreposer de l'information. Après quoi, une preuve du comportement cyclique s'est formée à la fin des années 90[13]. Une nouvelle inversion du marché des ventes des équipements informatiques est venue intensifier l'image d'une « centralisation hybride » qui fût décrite par certains auteurs[14] comme étant l'éveil des compagnies ayant compris le but précis des ordinateurs centraux dans l'économie traditionnelle des services informatiques. L'histoire ne s'arrête pas là, bien sûr, puisque l'infonuagique est considérée comme un retour au modèle centralisé[15] où la puissance de calcul

---

[9] D. A. PEAK, et M. H. AZADMANESH, « Centralization/decentralization cycles in computing: Market evidence. », 1997 Information and Management 31(6), 303–317.
[10] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (ci-après « OQLF »), « Le grand dictionnaire terminologique », en ligne : <http://www.granddictionnaire.com/index.aspx> (consulté le 28 avril 2019) - « Ethernet » : « Protocole de transmission de données par paquets utilisé dans les réseaux locaux, qui permet d'atteindre différents débits qui peuvent varier selon le support employé. ».
[11] *Id*., « *token ring* » : « Réseau local présentant une topologie en anneau qui utilise un jeton comme moyen de transmission des données entre les ordinateurs. ».
[12] Jeremy REIMER, « Total Share: 30 Years of Personal Computer Market Share Figures », (15 décembre 2005) *Ars Technica*, en ligne : <https://arstechnica.com/features/2005/12/total-share/> (consulté le 28 avril 2019).
[13] D. A. PEAK, et M. H. AZADMANESH, préc., note 7, p. 314.
[14] *Id*., p. 316.
[15] D. SULLIVAN, préc., note 8.

et les ressources principales sont déplacées depuis les utilisateurs finaux vers un emplacement géré centralement. Est-ce vraiment un nouveau cycle, ou seulement une continuation de la centralisation hybride décrite par les auteurs Peak et Azadmanesh[16] ? Le temps répondra à cette question.

Comme nous l'avons évoqué, les raisons économiques peuvent amener les universités à reluquer l'infonuagique. Précision que, comme nous le verrons, des données de toutes sortes se retrouvent dans les universités. Toutes ces catégories d'informations sont omniprésentes dans toutes les sphères d'activités universitaires et elles se multiplient à une vitesse fulgurante, ce qui engendre des dépenses de grande envergure. Sous le modèle informatique traditionnel, les universités ont construit leurs propres centres de traitements informatiques conçus pour répondre à la demande de leurs chercheurs et de leurs étudiants. Le coût de ces infrastructures est important et croit constamment. Pour leur part, les grands fournisseurs d'infonuagique offrent plusieurs de leurs technologies gratuitement ou à fort escompte pour les universités. Les raisons économiques sont donc un aspect important poussant le monde universitaire à regarder l'offre de cette technologie. Avec la récente annonce du ministre Caire, précédemment cité, le gouvernement du Québec estime que : « Cette centralisation doublée d'une dématérialisation devrait permettre de réaliser des économies de l'ordre de 100 millions de dollars […] »[17].

Comme nous le constatons, la politique influence aussi certainement l'engouement vers l'infonuagique. Bien entendu, cet enthousiasme est principalement d'intérêt économique. Par contre, il ne doit pas avoir lieu sans bien analyser les problématiques susceptibles de bouleverser l'information détenue par l'état et du même coup celles que possèdent les universités. Plusieurs questions peuvent être soulevées : est-il plus sécuritaire de conserver nos données localement ? Devons-nous préconiser des systèmes infonuagiques hybrides offerts par des fournisseurs gouvernementaux basés à même les réseaux des universités ?[18] Est-il préférable de favoriser l'hébergement au Canada ? Doit-on craindre l'infonuagique pour la conservation de renseignements personnels ou pour les droits de propriété intellectuelle ?

---

[16] D. A. PEAK, et M. H. AZADMANESH, préc., note 7, p. 314.
[17] D. JUNG, préc., note 5.
[18] Voir notamment, les Services infonuagique de Calcul Canada en ligne : <https://docs.computecanada.ca/wiki/Cloud/>.

Comme l'a rappelé Pierre Trudel en entrevue le 8 janvier de l'année courante, « Les données sont le pétrole du 21e siècle. »[19] . Est-ce alors une bonne idée, en plus de fournir d'emblée des informations personnellement au géant de l'informatique par l'utilisation de leurs services, d'y ajouter les données émanant de nos établissements d'enseignement ? Ne servons-nous pas leur cause (la course aux données) en transférant nos infrastructures informatiques dans leurs centres de données ?

En dépit de réponses claires à ces questions, nous devons encadrer juridiquement l'utilisation de l'infonuagique, et cette intervention ne peut provenir que par l'analyse des lois. Ces dernières ont joué et jouent encore un rôle majeur quant à l'importance de la protection de l'information dans nos vies. Bien évidemment, les universités ne sont pas indifférentes à cette science hétéronome.

Lors de l'adoption de la *Loi concernant le cadre juridique des technologies de l'information*[20] (ci-après « LCCJTI ») en 2001, le législateur québécois a voulu « assurer la validité et la sécurité des échanges […], peu importe le véhicule utilisé pour échanger. »[21]. Est-elle suffisante pour protéger nos informations de l'engouement des universités pour l'infonuagique ? Afin d'amenuiser les répercussions de ces technologies sur la protection de nos renseignements personnels, la *Loi sur l'accès aux documents des organismes publics et les renseignements personnels*[22] (ci-après « *Loi sur l'accès* ») ainsi que la *Loi sur la protection des renseignements personnels dans le secteur privé*[23] (ci-après « LPRPSP ») viennent, en corrélation avec la LCCJTI, cintrer les requis quant à la protection des données.

Bien entendu, tout développement technologique aura des incidences sur le droit. Évidemment, l'absence de jurisprudence sur ce sujet au Québec rend les répercussions du passage à l'infonuagique difficile à délimiter. Nous avons donc choisi d'étudier les textes

---

[19] Pierre Trudel (entrevue de Mathieu Beaumont), « Les données personnelles: enjeu majeur. » FM 98.5 Puisqu'il faut se lever, 8 Janvier 2019., en ligne : <https://www.985fm.ca/extraits-audios/opinions/180324/entrevue-me-pierre-trudel>.
[20] *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1.
[21] Robert CASSIUS DE LINVAL, « *Loi concernant le cadre juridique des technologies de l'information, Une innovation législative majeure* » Journal du Barreau du Québec, Volume 33 numéro 17, 2001.
[22] *Loi sur l'accès aux documents des organismes publics et les renseignements personnels*, L.R.Q., c. A-2.1.
[23] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1.

législatifs en vigueur afin de répondre à la question suivante : quel est le cadre juridique applicable à une infrastructure sous forme de service dans le milieu universitaire ?

Pour répondre à cette question, ce mémoire a été divisé en deux sections. Tout d'abord, dans le premier chapitre plus technique, nous avons utilisé le fondement de nos connaissances des technologies de l'information pour bien expliquer au lecteur la définition, les caractéristiques et le fonctionnement des différents systèmes infonuagiques. Le premier chapitre de ce mémoire sera suivi du cadre sécuritaire et des obligations de sécurité liées à l'utilisation des infrastructures sous forme de service par le milieu universitaire. Afin de bien interpréter la possibilité de l'impartition, nous croyons que nous devons, avant toute chose, connaître la composition de l'information se trouvant dans nos universités ainsi que ses degrés de classification. Aussi, afin de bien analyser l'obligation de sécurité prévue, nous avons élaboré, dans ce chapitre, une liste des risques les plus fréquemment encourus lors du passage vers les technologies infonuagiques. De plus, vous trouverez dans ce chapitre, avec un complément en annexe à ce mémoire, une analyse de risque sommaire sur laquelle le lecteur pourra se référer.

Dans la seconde partie, nous analyserons le cadre juridique et les obligations liées à l'utilisation de l'infrastructure sous forme de service relativement aux lois applicables aux institutions publiques. Puis dans un deuxième temps, aux règles ciblant les liens avec le privé, bien présentes dans le milieu universitaire.

Il s'agit d'un axiome fondamental que le droit réglemente et protège notre information. Il existe tout de même, au sein des institutions d'enseignement supérieur québécoises, beaucoup de souplesse quant à l'administration et la conduite des affaires académiques. Ainsi, « à moins de circonstances exceptionnelles, les tribunaux n'interviennent pas dans le fonctionnement interne des établissements universitaires qui jouissent traditionnellement d'une très grande autonomie »[24]. Cette autonomie ne doit tout de même pas se faire au détriment des obligations

[24] *Addy* c. *Commission scolaire Eastern Township*, 2010 QCCS 1708; voir aussi une mention à cet effet de la part du juge Trudel dans l'affaire *Aubin* c. *Université du Québec à Montréal,* 1997 QCCS 8773 mentionnant une décision de la cour d'appel à l'effet qu' « Il est un principe constant et bien reconnu en droit administratif canadien et québécois que les tribunaux de révision judiciaire ne s'immiscent pas dans les activités académiques et le fonctionnement interne des institutions d'enseignement […] ».

de sécurités informationnelles, soit la confidentialité, l'intégrité et la disponibilité des données qui seront la prémisse de notre analyse.

Nous admettrons que le domaine des technologies de l'information apporte son lot de néologismes. Le développement fructueux, en lien avec cette économie, ne se fait pas sans une nouvelle langue pour aller de pair avec elle. Nous avons tout de même simplifié, dans la mesure du possible, le langage technique utilisé afin de permettre une compréhension des enjeux liés au développement de l'infonuagique.

# PREMIÈRE PARTIE : Le cadre technologique relatif aux infrastructures en tant que service

# Chapitre I. Définir l'infonuagique

Avant de faire l'examen du cadre juridique applicable à une infrastructure sous forme de service dans le milieu universitaire, il est essentiel de bien définir ce qu'est l'infonuagique et d'identifier ses principales caractéristiques. Ainsi, puisque ce modèle informatique comporte de nombreux modes de déploiement et un nombre immesurable de types de ressources accessible à ses utilisateurs, leurs compréhensions seront essentielles afin de déterminer les risques découlant de leur exploitation. Les conséquences de leurs utilisations impliquent indéniablement une perte de contrôle sur les données et sur la sécurité de l'information. Nous évaluerons les obligations découlant du modèle qui nous intéresse à la deuxième section de la première partie de ce mémoire.

## 1.1 La définition et les caractéristiques des services infonuagiques

Afin de bien saisir le cadre législatif relatif aux infrastructures infonuagiques et d'en expliquer la portée, il est essentiel de comprendre correctement les particularités propres à ce concept ainsi que ses différents mécanismes de fonctionnements. L'infonuagique est une notion très vaste et couvre en toute vraisemblance une multitude de service en lignes que nous utilisons tous, sans nécessairement en avoir connaissance. L'expression « *Cloud computing* » provient des premiers temps de l'Internet où l'habitude était prise de dessiner le réseau comme un nuage afin de désigner une grande agglomération d'objets dont les détails sont plus ou moins inspectés dans un contexte donné[25]. Ainsi, contrairement à d'autres néologismes du Web 2.0[26], l'infonuagique est loin d'être éphémère.

---

[25] Pranay SANGHAVI, «why do we use a cloud as the shape to represent things like SkyDrive, iCloud, etc.?», *Quora*, 1er Février 2015, en ligne : <https://www.quora.com/Why-do-we-use-a-cloud-as-the-shape-to-represent-things-like-SkyDrive-iCloud-etc>, (consulté le 28 avril 2018)

[26] OQLF., préc., note 10, « Web 2.0 » : « Web doté d'outils et de contenus interactifs qui permettent aux internautes de participer à la création de contenus Web, de partager de l'information en ligne et de communiquer entre eux. ».

L'infonuagique est un paradigme en constante évolution, nous ne pourrons donc pas définir ce concept technologique comme étant nouveau. Sa compréhension est néanmoins souvent limitée aux services les plus connus et c'est la raison pour laquelle nous devons ensemble convenir d'une définition. Aux fins de ce mémoire, nous utiliserons celle émise par le National Institute of Standards and Technology (ci-après « NIST ») qui selon nous est l'une des sources les plus crédibles en matière d'innovation et de technologies :

> « *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.* » [27].

## 1.2 Les caractéristiques de l'infonuagique

De manière générale, l'opinion collective des systèmes infonuagiques ne diffère que peu des systèmes informatiques traditionnels. Néanmoins, la définition de l'infonuagique selon le NIST aux États-Unis stipule cinq caractéristiques essentielles propres aux systèmes informatiques en nuage[28] soit : le libre-service sur demande, l'accessibilité aux ressources, le regroupement de ressources, l'adaptabilité et la mesurabilité, lesquels nous aborderont maintenant. Cela dit, le processus mutationnel de l'infonuagique mène assurément à l'établissement de nouvelles caractéristiques. Même si elles ne sont pas officiellement reconnues par le NIST leurs immixtions sont inévitables selon nous. D'autres auteurs partagent également cette opinion[29]. C'est pourquoi nous ajouterons la « résilience » aux cinq caractéristiques sélectionnées par le NIST.

---

[27] Peter MELL and Timothy GRANCE, «The NIST definition of Cloud Computing», National Institute of Standards and Technology (ci-après « NIST»), September 2011, en ligne : <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> (consulté le 28 avril 2019).
[28] *Id*.
[29] Thomas ERL, Zaigham MAHMOOD, Ricardo PUTTINI, *Cloud Computing: Concepts, Technology & Architecture*, Upper Saddle River, Prentice Hall, 2013, page 61

### 1.2.1 Le libre-service sur demande

L'infonuagique permet à son consommateur d'accéder unilatéralement aux ressources informatiques dont il a besoin sans avoir nécessairement à interagir avec le service après-vente du fournisseur. Cette approche est contraire aux modèles informatiques traditionnels, où le besoin de ressources informatiques supplémentaires requiert inévitablement une acquisition de matériels, des installations de système d'exploitation, des migrations ainsi qu'une convergence avec les systèmes déjà en place, etc. Il pourrait, par ailleurs, même voir à automatiser l'allocation de ressources additionnelles ou moindres selon des paramètres préétablis.

### 1.2.2 L'accessibilité aux ressources

L'accessibilité aux ressources devrait nécessairement être effectuée via un réseau et être possible depuis une multitude de périphériques. Cette accessibilité devra également pouvoir se faire selon des mécanismes et des protocoles « standards »[30]. Somme toute, l'accès et la disponibilité des services infonuagique via une connexion Internet font en sorte que les services sont disponibles partout où se situe le client. Cette fonction permet notamment un accès à la portion infonuagique de l'infrastructure informatique (en cas de situation d'urgence, etc.) et facilitera l'accès ainsi que la collaboration depuis plusieurs emplacements.

### 1.2.3 Le regroupement de ressources

Le *regroupement de ressources* est un facteur clé afin de réduire les frais d'exploitation pour les fournisseurs de service infonuagique. Ce modèle mutualisé permet d'allouer des ressources physiques et virtuelles dynamiquement à un ou plusieurs consommateurs en fonction de leurs besoins. Depuis quelques années déjà, la virtualisation des infrastructures informatiques permet une telle optimisation, mais plus récemment, c'est l'hyperconvergence[31] qui permet une consolidation et ouvre la porte à de plus grosses infrastructures partageable. Nonobstant l'intégration de ces incommensurables ressources, il est primordial de discerner l'importance

---

[30] Raj SAMANI, Jim REAVIS and Brian HONAN, *CSA Guide to Cloud Computing, Implementing Cloud Privacy and Security*, Waltham, Syngress, 2014, p. 3.

[31] OQLF., préc., note 10, « hyperconvergence » : « Infrastructure informatique qui permet d'intégrer, à l'aide de logiciels, le stockage, la mise en réseau et les mécanismes de virtualisation dans une même architecture. ».

attribuée au « *tenant* » [32] ainsi qu'au « *tenant-multiple* » [33]. Qui plus est, certains technologues[34] scindent « le regroupement des ressources » en deux caractéristiques distinctes, soit le « regroupement » simplement et « l'utilisation des mêmes ressources par plusieurs groupes de consommateurs » (*multi-tenancy*). De notre côté, nous ne percevons aucunement l'utilité de les traiter séparément puisque la mise en commun des ressources amène inévitablement le partage de celles-ci.

### 1.2.4 L'adaptabilité

Afin de répondre à la demande des consommateurs infonuagiques, les ressources informatiques exploitées doivent s'adapter aux variations des charges imposées, c'est ce qu'on appelle le « service à la demande ». Pour les consommateurs, les fonctionnalités disponibles pour l'approvisionnement paraîtront comme illimitées et pourront être obtenues à tout moment. Cette allocation dynamique est un mécanisme qui permet aux administrateurs de définir des politiques sur l'utilisation des ressources dynamiquement allouées depuis un plus grand bassin agrégé, selon l'utilisation réelle du client. Bien entendu, ils pourront par ailleurs être dans certains cas automatisés.

### 1.2.5 La mesurabilité

L'utilisation des services et des ressources est surveillée, contrôlée, administrée, mesurée et elle sera inévitablement facturée au consommateur. Les audits constants assureront une transparence autant pour le fournisseur que pour l'acquéreur du service. Ils permettront

---

[32] T. ERL, Z. MAHMOOD, R. PUTTINI, préc., note 29, p. 370; Ian FELDER, «SaaS : Single Tenant vs Multi-Tenant – What's the Difference?», *DataInsider Digital Guardian's Blog*, 26 Avril 2019, en ligne : < https://digitalguardian.com/blog/saas-single-tenant-vs-multi-tenant-whats-difference>, (consulté le 28 avril 2019) : Un tenant se défini comme : « *A single instance of the software and supporting infrastructure serve a single customer. With single tenancy, each customer has his or her own independent database and instance of the software. Essentially, there is no sharing happening with this option.* ».

[33] *Id*., p. 106-107.; Ian FELDER, «SaaS : Single Tenant vs Multi-Tenant – What's the Difference?», *DataInsider Digital Guardian's Blog*, 26 Avril 2019, en ligne : <https://digitalguardian.com/blog/saas-single-tenant-vs-multi-tenant-whats-difference>, (consulté le 28 avril 2019). : Un multi-tenant se défini comme : «*Multi-tenancy means that a single instance of the software and its supporting infrastructure serves multiple customers. Each customer shares the software application and also shares a single database. Each tenant's data is isolated and remains invisible to other tenants.* ».

[34] San MURUGESAN, Irena BOJANOVA, *Encyclopedia of Cloud Computing*, Chichester, Wiley-IEEE Press, 2016, p. 5 et suivante.

également d'assurer une coordination entre la capacité des systèmes ainsi que les ententes de services pris entre les parties.

### 1.2.6 La résilience

Le concept de résilience est une caractéristique majeure en infonuagique. Utilisant des principes de basculement[35] informatique, ce principe de continuité signifie qu'il y a un jeu distribué des ressources sur le réseau qui permettra d'augmenter la disponibilité et la fiabilité des services. Si une ressource tombe en panne, le système redirigera automatiquement les requêtes vers un système de relève sans que les utilisateurs en aient conscience.

## 1.3 Les modèles de déploiement infonuagiques

Il existe plusieurs modèles de déploiement pour l'infonuagique. Ces modèles sont en fait des stratégies différentes permettant toutes d'arriver à l'implémentation d'un système d'information dit « dans les nuages »[36]. Chaque modèle comporte ses avantages et ses inconvénients, mais ils sont tous basés sur la valeur de leur droit de propriété et de leurs degrés de partages[37]. Ainsi, comme nous le verrons, la sélection d'un mode de déploiement infonuagique aura de grandes répercussions sur la sécurité de l'information et sur la disponibilité des données. Par ailleurs, les modèles disponibles n'énoncent en aucun temps les niveaux minimums auxquels il devrait faire référence. Comme le mentionne le NIST :

> « […] *While the choice of deployment model has implications for the security and privacy of a system, the deployment model itself does not dictate the level of security and privacy of specific cloud offerings. That level depends mainly on assurances, such as the soundness of the security and privacy policies, the robustness of the security and privacy controls, and the extent of visibility into performance and management details of the cloud environment, which are*

[35] OQLF., préc., note 10, « Basculement » : « Dispositif qui, en cas de panne, assure l'intégrité et la disponibilité des données, par leur transfert, sans interruption de service, du composant informatique où elles se trouvent à un composant auxiliaire. ».
[36] *Id*, préc., note 7.
[37] R. SAMANI, J. REAVIS et B. HONAN, préc., note 30, p.5.

*furnished by the cloud provider or independently attained by the organization (e.g., via independent vulnerability testing or auditing of operations).* »[38].

### 1.3.1 Le modèle public

Lorsqu'il est question d'infonuagique, le modèle public est généralement référencé. La raison est toute simple : les services les plus connus et populaires sont de nature publique[39]. Le « Public Cloud » se dit lorsque le modèle de déploiement est mis à la disposition du grand public par l'entremise du réseau Internet[40]. Ce service est offert à l'externe de l'entreprise, généralement par des compagnies, des universités ou encore des gouvernements[41] possédant d'importantes infrastructures leur permettant de jouer le rôle de fournisseur de services. De manière habituelle, ces clients ne sont pas nécessairement liés et ils ne font pas partie d'une même et unique organisation. Même s'il en était autrement, ils ne seront généralement pas au fait des autres utilisateurs du même service, puisque la nature même du modèle public est qu'il est disponible à tous.

Bien entendu l'avantage le plus imposant du modèle public sera l'économie financière, puisque les dépenses en immobilisations (serveurs, stockages[42], licences, infrastructure informatique, etc.) seront désormais remplacées par des dépenses d'exploitation. Les coûts opérationnels et celui des services aux utilisateurs seront en effet diminués dans la mesure où le consommateur des nuages public paye selon son utilisation[43]. L'évolutivité possible pour répondre aux demandes ponctuelles de ressources supplémentaires limitera également les dépenses impromptues. L'équilibrage géographique offre un accès rapide et assuré en tous lieux aux données de l'entreprise, il permettra une simplification de la collaboration entre les employés, et proposera une amélioration de la résistance aux désastres naturels[44]. Les grands fournisseurs de service infonuagique seront réfractaires à en parler, mais ils ont néanmoins été

---

[38] Wayne JANSEN et Timothy GRANCE, « Guidelines on Security and Privacy in Public Cloud Computing », NIST, Décembre 2011, en ligne : <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf >, p. 4., (consulté le 28 avril 2019).
[39] R. SAMANI, J. REAVIS and B. HONAN, préc., note 30, p. 5.
[40] P. MELL et T. GRANCE, préc., note 27, p. 3.
[41] *Id*.
[42] OQLF., préc., note 10, « Stockage » : « Conservation des données dans une mémoire. »
[43] S. MURUGESAN, I. BOJANOVA, préc., note 34 p. 11.
[44] *Id*., p. 10.

victimes de tentatives de piratage continues depuis plusieurs années[45]. Malgré que cet élément pourrait paraître un désavantage, il n'en demeure pas moins que ces fournisseurs de services ont, depuis ce temps, non seulement acquis les ressources matérielles pour se prémunir contre ces actions, mais ils ont recruté également les meilleurs experts en sécurité pour pallier ces attaques[46]. Peu de compagnies peuvent en dire autant de leur investissement en sécurité de l'information[47]. Les grands fournisseurs de services infonuagiques auront par défaut une sécurité accrue en comparaison à ce que la plupart des entreprises peuvent se permettre dans leur propre centre de données. Pour pallier le besoin criant de sécurité de l'information, depuis le 1er novembre 2018, les organisations assujetties à la « *Loi sur la protection des renseignements personnels et les documents électroniques* »[48] ci-après LPRPDÉ doivent maintenant « déclarer au commissaire à la protection de la vie privée du Canada les atteintes aux mesures de sécurité concernant des renseignements personnels présentant un risque réel de préjudice grave à des individus. »[49]. Toutefois, ce n'est pas le cas des universités.

Malgré cela, la sécurité des données détenues dans le nuage demeure néanmoins le facteur le plus préoccupant au passage vers ces technologies. Cela dit, il est souvent vu comme un avantage que le nuage public n'ait aucune restriction géographique facilitant ainsi l'accès de partout où nous sommes. Inversement, cette commodité pourrait signifier que votre service infonuagique public se trouve dans un autre pays et donc, avec une juridiction différente[50]. De plus, puisque les services sont dispensés par l'intermédiaire d'Internet, le modèle public se verra être opéré à l'extérieur des frontières informatiques de l'organisation utilisant le service. Il

---

[45] Par exemple, en 2014, le service iCloud de Apple a été la proie de « hacker » et des centaines de photos de célébrités se sont retrouvés en ligne par suite de lacunes du service ou de mauvaise habitude des utilisateurs de la plateforme. Voir notamment Jennifer Lawrence, « Photos piratées de stars : Tous les utilisateurs de clouds doivent-ils être inquiets? », (19 septembre 2014), *AFP – 20 Minutes*, en ligne : <https://www.20minutes.fr/high-tech/1435971-20140902-photos-piratees-stars-tous-utilisateurs-clouds-doivent-etre-inquiets >, (consulté le 29 avril 2019).

[46] R. BALASUBRAMANIAN, M. ARAMUDHAN, « Security Issues: Public vs Private vs Hybrid Cloud Computing», *International Journal of Computer Applications*, volume 55- No.13, Octobre 2012 p. 37.

[47] Conclusion #226, 2003 48376 (C.V.P.C.).

[48] *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5).

[49] C.V.P.C., « Comment réagir à une atteinte à la vie privée dans votre entreprise », en ligne <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/>, (consulté le 28 avril 2019).

[50] Le cas le plus médiatisé étant United States v. Microsoft Corp., No. 17-2, 584 U.S. (2018).

faudra sans aucun doute délester quelques règles de coupe-feu[51] afin de s'assurer du bon fonctionnement du réseau Internet et indubitablement augmenter la bande passante du réseau de l'entreprise.

Une dépendance implicite, également connue sous le nom « vendor lock-in »[52], constitue un autre inconvénient de l'infonuagique. Les différences profondes entre les systèmes hétérogènes des grands exploitants de service infonuagique peuvent parfois rendre impossible la migration de plate-forme d'un nuage public à l'autre. Non seulement il est complexe et coûteux de reconfigurer vos applications, vos plateformes ou vos infrastructures pour répondre aux exigences d'un nouvel hôte, mais la migration pourrait aussi exposer vos données sensibles à des risques pour leur sécurité ainsi qu'à des vulnérabilités transitoires. Plusieurs types d'« *enfermements* » peuvent survenir[53]. Un enfermement de plateforme ou d'infrastructure vis-à-vis une technologie utilisée pourrait être par exemple :

- une technologie spécifique de virtualisation,
- un outil de gestion particulier ou plus pernicieusement, ou
- un confinement des données.

D'où la question : qui possède ultimement les données entreposées dans les nuages ? Ici, il est question de permanence des données, nous y reviendrons subséquemment.

Comme mentionné auparavant, le dessin du nuage représente un ensemble dont les détails internes nous sont inconnus. Il s'agit immanquablement de la situation du modèle public. Il sera impossible pour un client d'obtenir une divulgation des données relatives aux infrastructures du fournisseur ou d'en connaître le fonctionnement interne. À moins d'une mention explicite au contrat de service, rien n'empêche un fournisseur de service infonuagique d'impartir à son tour l'un ou l'autre des éléments constituant l'infrastructure offerte aux

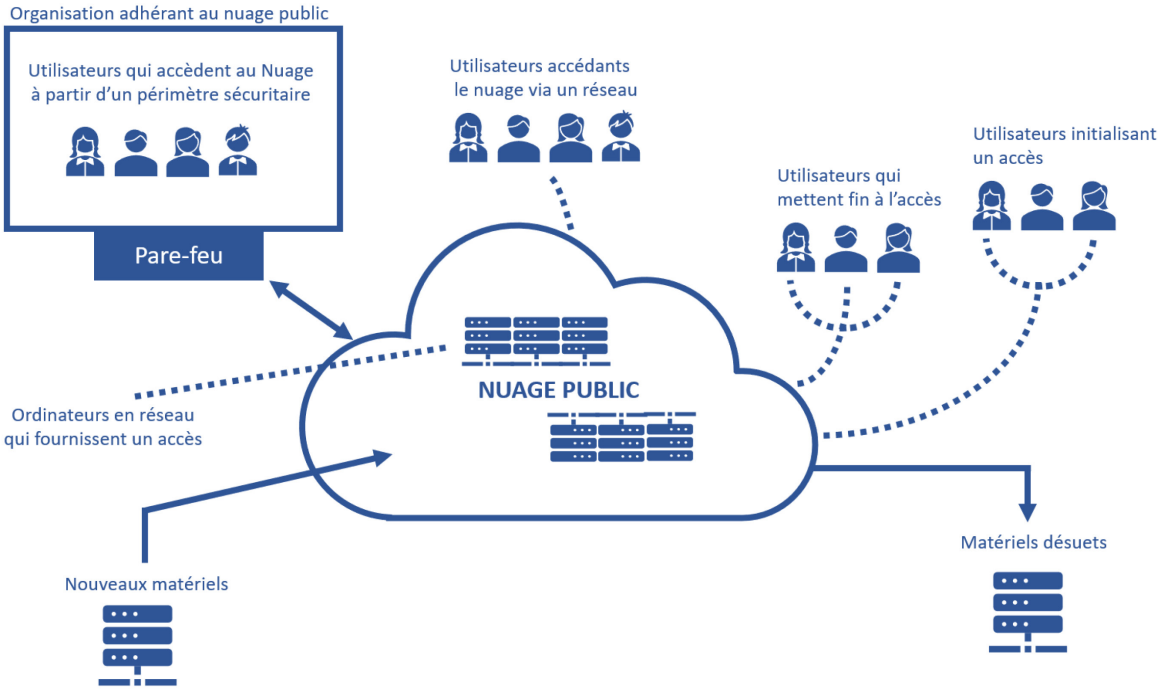
---

[51] OQLF., préc., note 10, « coupe-feu » : « Dispositif informatique qui permet le passage sélectif des flux d'information entre deux réseaux, ainsi que la neutralisation des tentatives de pénétration extérieures. ».
[52] Enfermement propriétaire de l'anglais « *Vendor lock-in* », « est la situation dans laquelle des clients sont tributaires d'un seul fabricant ou fournisseur pour certains produits ou service, et où il est impossible de revenir à un autre fournisseur sans d'énorme inconvénients et des coûts substantiels. ».
[53] R. SAMANI, J. REAVIS, B. HONAN, préc., note 30, p. 18.

clients[54]. Bien entendu, les fournisseurs de services infonuagiques offriront des visites guidées de leurs locaux, et permettront même que des « tests d'intrusion »[55] de leurs systèmes soient effectués par une tierce partie, après notification de la part du client[56]. Même si elles le permettent, ces audits seront limités à un examen de leur politique et de leur procédure sans égard à l'efficacité de leur mise en œuvre.

Finalement, l'utilisation du modèle infonuagique public mènera inévitablement à une perte d'autonomie envers l'évolution de certaines des solutions technologiques disponibles et des possibilités qu'offrent les technologies de l'information[57]. En effet, la compétence interne de l'entreprise et les connaissances des systèmes ne pourront facilement suivre les mutations du milieu s'ils sont gérés par un prestataire de service externe à l'entreprise.

Figure 1. Modèle public




[54] Nicolas W. VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », Centre de recherche en droit public, Université de Montréal, mars 2014, p. 56.
[55] OQLF., préc., note 10, « tests d'intrusion » : « Test au cours duquel un spécialiste tente de pénétrer dans un réseau de systèmes informatiques dans les mêmes conditions qu'un intrus éventuel, afin de vérifier l'efficacité des dispositifs de sécurité mis en place et d'éliminer les failles décelées grâce à cette opération. ».
[56] Voir notamment les règles d'engagements de Microsoft, en ligne : <https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1>.
[57] W. JANSEN et T. GRANCE, préc., note 38, p. 40.

### 1.3.2 Le modèle privé

Le modèle privé, « Private Cloud », se dit d'une structure informatique exploitée pour un seul organisme[58] qu'elle soit administrée à l'interne de ce même organise ou à l'externe par une partie tierce[59]. Il s'agit en fait d'un réseau informatique traditionnel, opéré sous forme de virtualisation sur une grappe de serveurs, où les échanges de communications sont généralement isolés des réseaux publics. Le modèle privé permettra l'accès aux ressources seulement aux utilisateurs autorisés et connus d'une entreprise. Ce modèle permet un plus grand contrôle sur l'infrastructure ainsi que sur les données, comme nous le verrons ci-après.

Le principal avantage du modèle privé est un plus grand niveau de sécurité. Effectivement, le modèle privé sera « déployé, disponible et contrôlé par une entreprise derrière son coupe-feu, pour [son] usage propre »[60]. Il en sera ainsi que le modèle soit délivré depuis l'interne ou depuis l'externe, à la seule différence que lorsqu'il sera administré à l'externe, il devra communiquer avec l'infrastructure locale par la voie de liens réseau privés ou de connexions sécurisées par chiffrement via un réseau public. Le résultat sera un prolongement des mesures de sécurité du réseau local à la partie dans les nuages.

Comme l'accès à l'infrastructure est privé, la mise en place des normes, des procédures ainsi que la gestion des accès aux utilisateurs déjà en vigueur dans l'entreprise seront facilités et pourront être modifiés aisément[61]. Il sera également possible contrairement au modèle public de voir à appliquer, surveiller, et auditer les services, lorsque requis par le type d'entreprise[62]. « De cette manière, l'organisation peut plus facilement se conformer aux règles relatives à la protection des renseignements et être en mesure de démontrer les mesures prises à cet effet. »[63].

Le client utilisant le service infonuagique privé pourra garder le contrôle sur l'emplacement géographique de ces données[64]. De plus, s'il choisit de décentraliser une partie

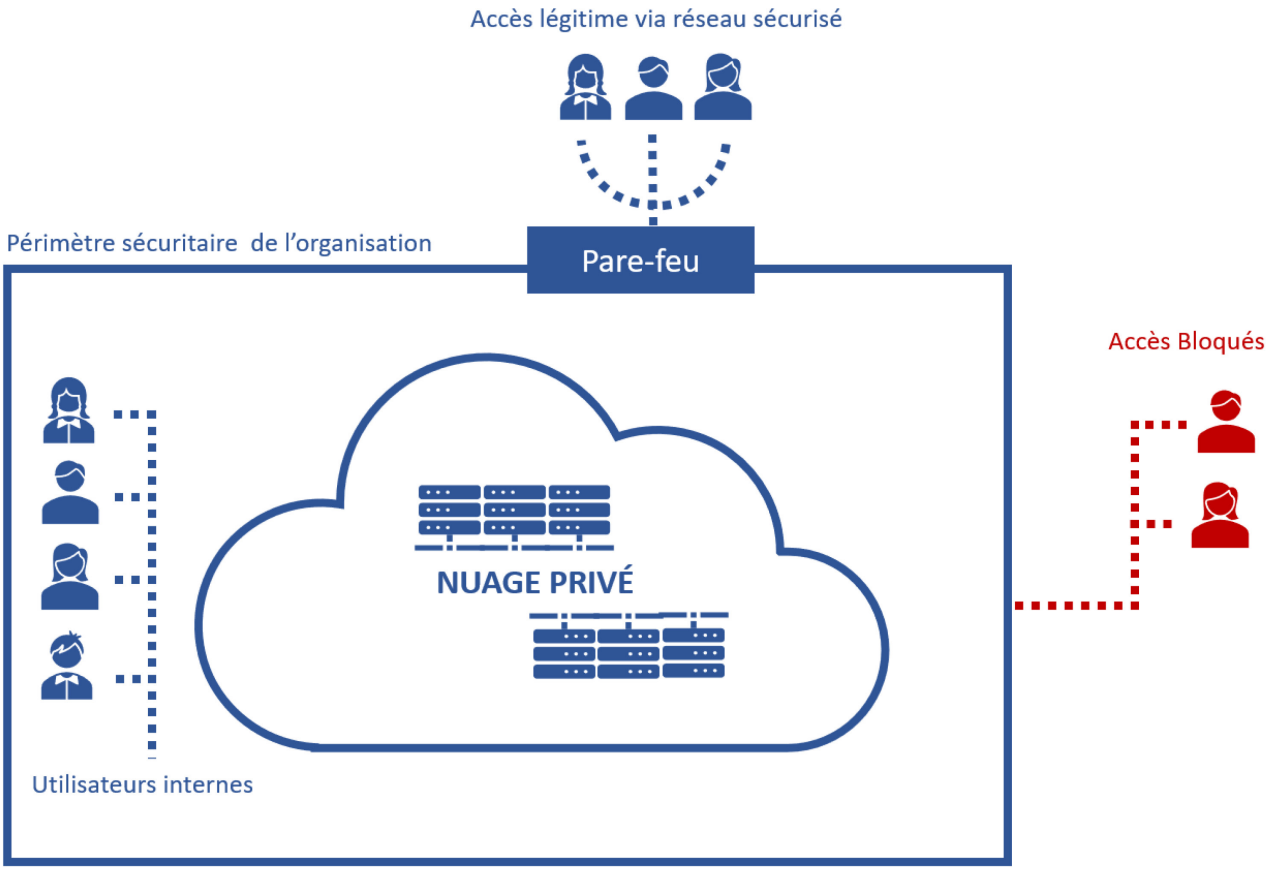
---

[58] R. SAMANI, J. REAVIS et B. HONAN, préc., note 30, p. 6.
[59] P. MELL et T. GRANCE, préc., note 27.
[60] S. MURUGESAN et I. BOJANOVA, préc., note 34, p. 9.
[61] R. SAMANI, J. REAVIS et B. HONAN, préc., note 30, p. 6.
[62] Rajkumar BUYYA, James BROBERG, Andrzej M. GOSCINSKI, « Cloud Computing Principles and Paradigms », Hoboken Wiley, 2011, chap. 9 p. 253.
[63] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 15-16.
[64] R. SAMANI, J. REAVIS et B. HONAN, préc., note 30, p. 6.

de son infrastructure hors site, il augmentera la résistance aux événements malencontreux pouvant se produire ainsi que sa tolérance aux pannes informatiques.

Lorsque confiné à l'interne, le modèle privé se verra être limité par les ressources locales de l'entreprise. En conséquence, les coûts de mise en place d'une infrastructure privée seront possiblement exorbitants et facilement exponentiels. Par ailleurs, afin de permettre des variations de charge à l'utilisation, l'entreprise se verra dans l'obligation de détenir une capacité informatique supérieure à ses besoins. De plus, sauf si nous avons recours à un service tiers, un nuage privé peut être difficile à mettre en œuvre en toute sécurité. Il s'avère alors indispensable d'avoir une équipe en TI spécialisés détenant une connaissance approfondie de la façon dont ces nuages peuvent être gérés et lier avec les besoins professionnels de l'organisation. Les besoins fréquents de maintenance et de mises à jour exerceront une pression additionnelle sur les technologues responsable de l'infrastructure et limiteront le temps disponible pour les tâches traditionnelles.

Figure 2. Modèle privé



### 1.3.3 Le modèle communautaire

Nonobstant l'émergence des différents services infonuagiques publics, il va de soi qu'ils ne correspondront pas nécessairement aux besoins spécifiques de certaines communautés d'utilisateur. C'est la raison pour laquelle un modèle aux caractères communautaire a été figuré. Le « *community cloud* », ou modèle communautaire, est comparable au nuage privé du point de vue de l'infrastructure[65]. Par contre, il joint différents organismes requérants les mêmes types d'architectures et ayant des préoccupations communes à ce qui a trait à leurs conformités, à leurs besoins de sécurités ainsi qu'à leurs réglementations internes. Chaque organisation participante peut fournir des services infonuagiques ainsi que les utiliser. Conséquemment, tout comme le nuage privé, ce modèle peut aussi être interne ou externe à l'organisation[66].

Une approche courante est qu'un fournisseur de service infonuagique public met en place une infrastructure distincte et développe des services spécifiques pour une communauté. Autrement, le modèle communautaire peut être aussi instauré par des membres de la communauté qui ont déjà une expertise dans le domaine et qui se réunissent pour fédérer leurs nuages privés.

Il n'en demeure pas moins que chaque « nuage communautaire » sera spécialisé selon des fonctionnalités et des caractéristiques particulières essentielles par sa communauté[67]. Ainsi, l'avantage réside dans la possibilité d'offrir des solutions optimisées à des communautés d'utilisateurs spécifiques, tout en réduisant les coûts, la gestion et l'opération de la sécurité reliés à un tel service.

Habituellement, chaque organisme utilisant l'infrastructure mise en commun disposera de son propre périmètre de sécurité puisque les données demeurent non partageables au sens propre. Comme les membres de la communauté dispose de similarité quant à leurs obligations de sécurité, les règles quoiqu'indépendante pourront être partagés. Malgré cette union, la

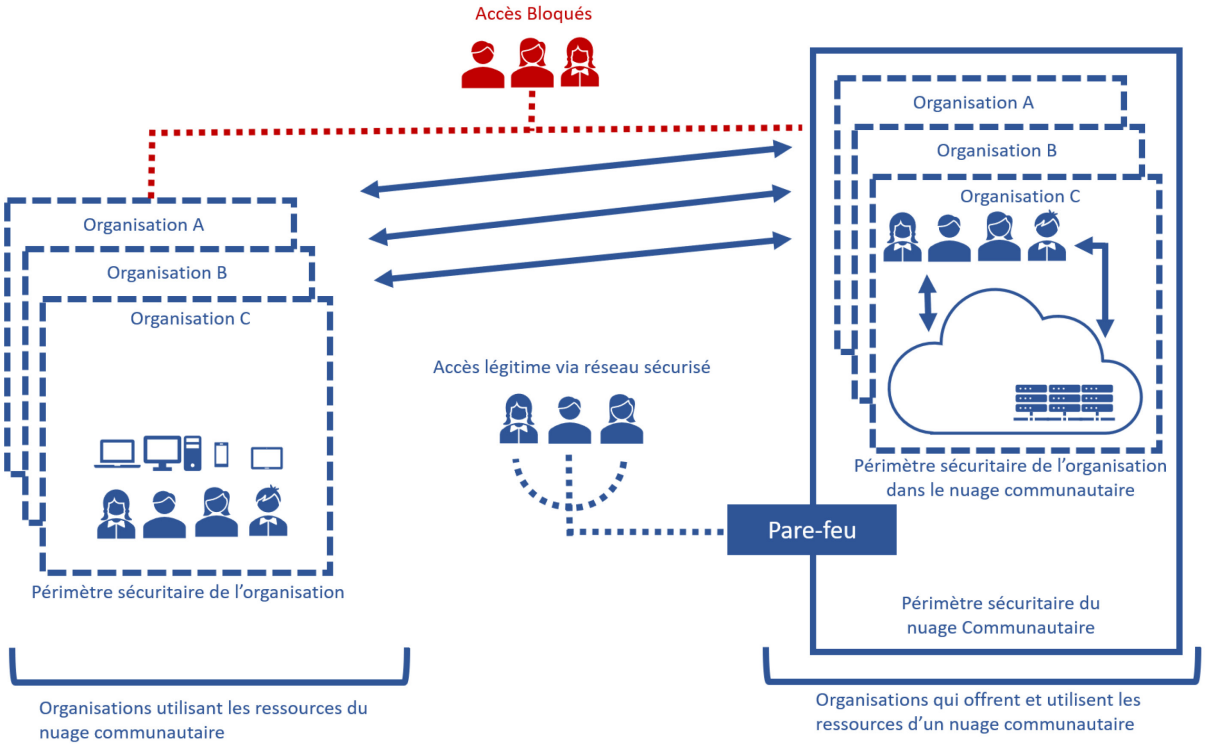
---

[65] P. MELL et T. GRANCE, préc., note 27, p. 3.
[66] Lee BADGER, Tim GRANCE, Robert PATT-CORNER et Jeff VOAS, « Cloud computing synopsis and recommendations », NIST, May 2012, en ligne : < https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf> (consulté le 28 avril 2019), p. 4-9.
[67] S. MURUGESAN et I. BOJANOVA, préc., note 34, p. 42.

nécessité de multiples liens sécurisés de communication augmentera les besoins et les coûts de bande passante[68].

Une complication majeure à ce système est que de nouvelles entités participantes peuvent joindre la communauté ainsi que la quitter. Au fil du temps, ces changements peuvent fragiliser et compliquer la pérennité du nuage.

Figure 3. Modèle communautaire




[68] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 4-12.

### 1.3.4 Le modèle hybride

Il peut y avoir également d'autres modèles de déploiement, tels que le modèle distribué ou le modèle hybride[69], qui sont des dérivés des grandes familles mentionnés ci-haut.

Dans cette approche, une organisation fera le choix d'utiliser plusieurs modes de fonctionnement afin d'atténuer les avantages et les inconvénients de chacun[70]. Les utilisateurs de modèle hybride pourront alors orchestrer leurs « utilisations » en fonction des caractéristiques de performance, de fiabilité et de sécurité recherchées. Bien entendu, puisqu'il implique une composition de plusieurs modèles, il s'avère plus complexe[71]. Il s'agit incontestablement de son plus grand désavantage.

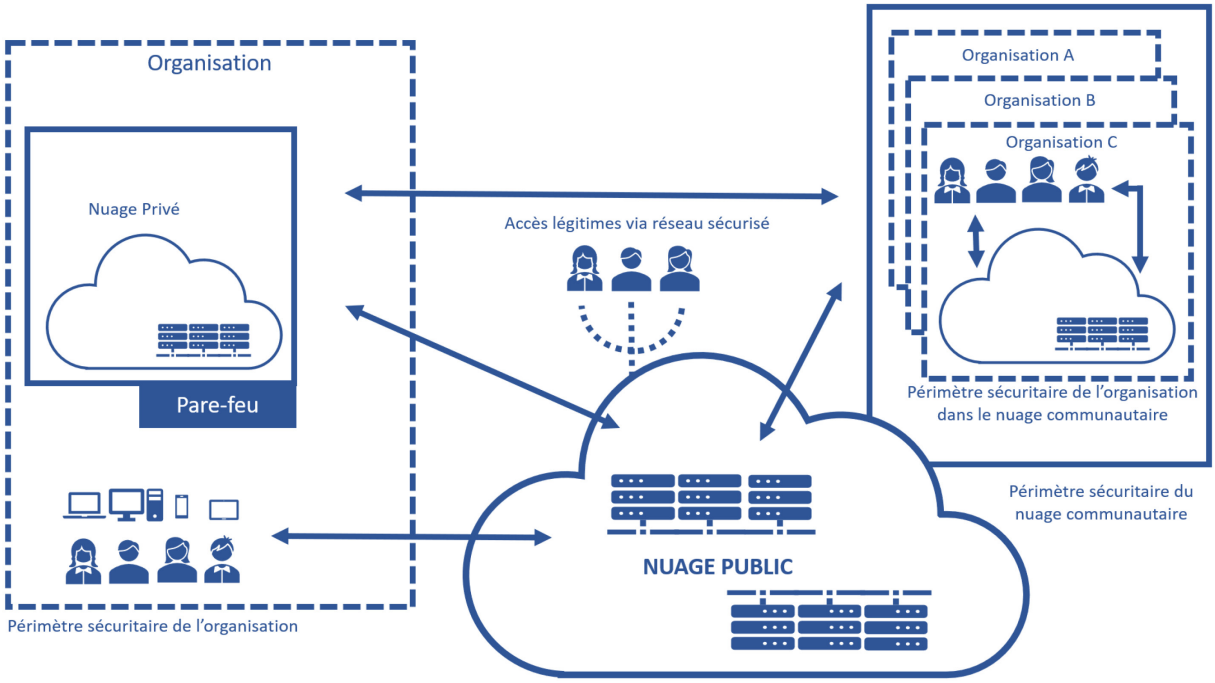
Le modèle hybride offrira, en revanche, l'avantage du coût et la disponibilité des ressources en grande quantité du modèle public, tout en offrant la sécurité et le contrôle des nuages privés. Il permettra notamment d'optimiser les différentes étapes du cycle de vie d'une application infonuagique. En effet, le modèle public peut être exploité pour le développement et les tests d'une application, puis à la fois permettre par la suite d'être porté au nuage privé de l'entreprise pour assurer la confidentialité des données requise lors de la production[72]. Il sera aussi possible d'effectuer un équilibrage des charges de travail excédentaire, et moins critique, dynamiquement pour accommoder les variations passagères[73]. Cette capacité se nomme « *cloud bursting* »[74]. Cette fonction permettra de faciliter les transferts de données d'un milieu privé à un milieu public. Néanmoins, il demeure essentiel que ces mouvements soient opérés dans le respect de la confidentialité ainsi que dans l'intégrité des données et des applications. Bien entendu, ces paramètres varient considérablement du nuage privé au nuage public.

---

[69] P. MELL et T. GRANCE, préc., Note 27.
[70] Richard HILL, Laurie HIRSCH, Peter LAKE, et Siavash MOSHIRI, *Guide to Cloud, Principles and Practice*, London, Springer, 2013, p. 12.
[71] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 4-16.
[72] Sumit GOYAL(2014) « Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review », I.J. Computer Network and Information Security 2014, 3, 20-29, p. 25. en ligne : <http://www.mecs-press.org/ijcnis/ijcnis-v6-n3/IJCNIS-V6-N3-3.pdf> (consulté le 28 avril 2019).
[73] Borko FURHT, and Armando ESCALANTE. *Handbook of cloud computing, Vol. 3*, New York, Springer, 2010, p. 68.
[74] Barrie SOSINSKY, *Cloud Computing Bible, Indianapolis*, Wiley, 2011, p. 304.

Cette hybridation étend le périmètre de sécurité à l'extérieur des limites organisationnelles, il s'avère augmenter les risques d'attaques et de failles de sécurité pour le segment du système sous le contrôle d'un prestataire de services offrant le nuage public. De plus, ce risque pourrait également s'étendre à la partie privée du nuage si des mesures de sécurité limitrophe ne sont pas adéquatement prises.

Figure 4. Modèle hydride




Il n'y a pas de solution unique pour tous, des choix doivent être faits lors de la sélection d'une méthode de déploiement. Une analyse de risque basé sur les besoins de l'entreprise[75], la rigueur des contrôles et des besoins de sécurités convoités est essentielle.

Ces méthodes de déploiement auront des répercussions tant au niveau du droit à la vie privée que de la sécurité de l'information[76], mais ne délimitent pas pour autant les frontières de sécurité nécessaires à leur mise en œuvre. Généralement, un contrat avec le prestataire de service

[75] Nicolas W. VERMEYS, *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010, p. 47.
[76] W. JANSEN et T. GRANCE, préc., note 38, page 4.

évoquera les différentes règles de gouvernance ainsi que les niveaux de sécurité requis à la gestion des technologies de l'information de l'entreprise.

## 1.4 Les modèles de prestation de services

Le concept de modèles de prestation de service indiquera le type de ressources auquel un utilisateur des services infonuagique aura accès. Subséquemment, la quantité de modèles de services infonuagique est en constante évolution. De là l'apparition du terme « N'importe quoi en tant que service », XaaS[77]. Aujourd'hui, des entreprises en technologie de toutes spécialités pourront offrir ce dont nous avons besoin « en tant que service ». Le CaaS[78], ou la « *communication as a service* », permet au consommateur d'utiliser des systèmes de téléphonique VoIP[79], de Réseau Privé Virtuel et des PBX[80] sans avoir à investir sur une infrastructure de communications unifiées. Le MaaS[81], ou le « *monitoring as a service* », offre la possibilité de surveiller l'état de différents services infonuagiques, en plus de faire l'analyse de journal d'évènement depuis un tableau de bord central basé sur le web. Le « *Desktop as a Service* » connu sous le DaaS[82], est une infrastructure de bureau virtuel (VDI) dans lequel un système d'exploitation client est externalisé et supporté par une partie tierce. Nous pourrions continuer ainsi, mais généralement, les experts s'entendent pour regrouper les différentes appellations dans trois principaux modèles de prestation de service connue sous « le modèle SPI » pour « *Software (1.4.1), Platform (1.4.2), Infrastructure (1.4.3)* »[83].

---

[77] On utilise l'achronyme «XaaS» pour exprimer « Anything as a Service», voir notamment, R. SAMANI, J. REAVIS and B. HONAN, préc., note 30, chap. 1 p. 7; Christopher MILLARD, *Cloud Computing Law*, Oxford, Oxford university Press, 2013, Abstract and Keyword.
[78] Siani PEARSON, George YEE, *Privacy and Security for Cloud Computing*, London, Springer, 2013, p. 60.
[79] OQLF., préc., note 10, « VoIP » : « Technique utilisant le protocole de l'Internet pour le transport de la voix sur un réseau de télécommunication. ».
[80] *Id.*, « PBX » : « Commutateur téléphonique qui, à l'intérieur d'une entreprise, gère de manière automatique les communications entre plusieurs postes et qui sert à établir celles avec l'extérieur. »
[81] S. MURUGESAN et I. BOJANOVA, préc., note 34, p. 9.
[82] *Id.*, p. 8.
[83] *Id.*, p. 7.

### 1.4.1 Le logiciel sous forme de service (SaaS)

Le terme « SaaS » fait référence au logiciel dans un nuage, c'est-à-dire une « Prestation de service proposant à un client l'utilisation à distance d'un logiciel et dont le coût correspond à son usage effectif. »[84]. Ce modèle est une proposition simple avec une souplesse très limitée pour le client[85]. Il s'agit du service infonuagique le plus complet, disponible sous forme d'application depuis un navigateur web. Il est aussi le plus vieux, il existait bien avant que le concept d'informatique dans les nuages émerge. Les services de courrier en ligne en sont un exemple typique, apparu un peu après les premiers balbutiements de l'Internet. Cela dit, nous y retrouvons maintenant une multitude d'applications. C'est le modèle infonuagique le plus utilisé puisqu'il comprend notamment les réseaux sociaux et les nombreuses applications de bureaux disponibles en ligne[86]. Il s'agit d'avoir un besoin, de trouver le bon logiciel qui répond à ce besoin, de l'essayer pendant une courte période, et d'en faire l'utilisation jusqu'à ce qu'ils ne répondent plus au besoin. Il est ainsi aisé de passer à une autre solution[87]. L'ensemble des composants physiques des systèmes, le contrôle de l'infrastructure, des systèmes d'exploitation et même du logiciel en soi sont évidemment, aucunement sous le contrôle ou la responsabilité de l'utilisateur[88]. Ce modèle ne sert qu'à rendre disponible une application. La seule responsabilité du client est d'y introduire des données et d'effectuer le traitement en interaction avec elles[89].

Le développement et la publication d'un logiciel sous forme de service sont une excellente alternative pour une multitude d'applications. Il n'y a plus aucun problème d'interopérabilité avec les différentes versions de plateforme à supporter, l'application réside directement sur le système du prestataire de service ou sur celui d'un tiers[90]. Cette centralisation

---

[84] OQLF., préc., note 10, « logiciel à la demande ».
[85] R. SAMANI, J. REAVIS et B. HONAN, préc., note 37, p. 8.
[86] Notons par exemples : Microsoft Office 365, Google G Suite, Adobe Creative Cloud, etc.
[87] R. HILL, L. HIRSCH, P. LAKE, et S. MOSHIRI, préc., note 70, p. 15.
[88] P. MELL et T. GRANCE, préc., note 27, p. 3.
[89] *Id*., préc., note 87, p. 97.
[90] *Id*.

permet également de simplifier les maintenances[91] et l'installation de rustines applicatives ou liées à la sécurité.

Le programmeur et le fournisseur du logiciel bénéficieront également d'une meilleure protection de leur propriété intellectuelle, puisque l'application n'est pas déployée puis distribuée largement et localement chez les utilisateurs[92]. Après tout, le consommateur n'obtient seulement qu'un droit d'utiliser l'application et la possibilité de gérer les données liées à celle-ci, telle que leurs sauvegardes et parfois leurs partages entre consommateurs[93]. Ce droit d'utilisation verra du même coup à réduire les frais de surapprovisionnement des licences associées aux logiciels, puisqu'une seule et même licence pourra être utilisée sur plusieurs ordinateurs à des moments différents[94]. Cette façon de faire permettra sans aucun doute une économie importante de coûts.

Comme nous venons tout juste de le mentionner, des données relatives aux logiciels infonuagiques doivent vraisemblablement être accessibles via l'application. Cet élément implique que les données transigeront depuis et vers l'infrastructure du prestataire de service. Ce mouvement d'information n'est pas à prendre à la légère, puisque les données qui transigent via un réseau situé à l'extérieur du pare-feu de l'organisation sont susceptibles d'être perdues ou interceptées. La mise en place de technologie de cryptage et de procédés de corrections d'erreur est généralement instaurée par le fournisseur de service, dans le cas contraire des mesures compensatoires devront être prises[95]. De plus, en s'appuyant sur le navigateur du consommateur pour l'accès à l'interface logiciels, l'approche SaaS déclenche évidemment un risque additionnel si le navigateur du client est contaminé par un logiciel malveillant, les données y transigeant pourraient alors être compromises[96].

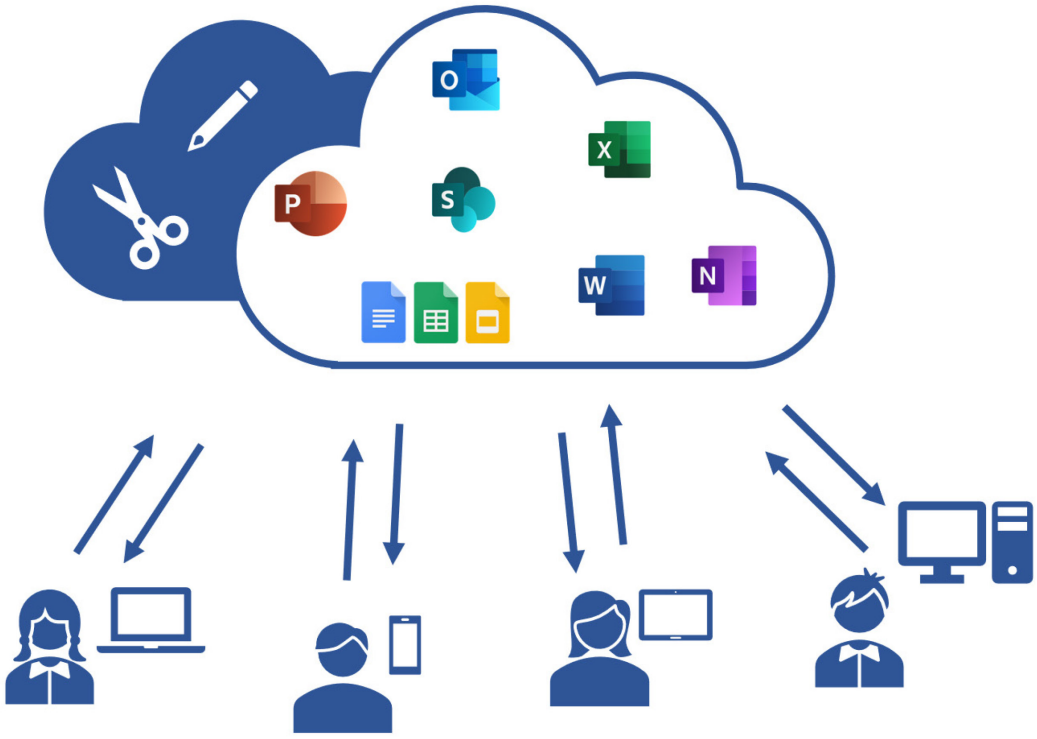
Une fois accessibles depuis l'application, les données sont à nouveau contraintes à des enjeux importants, particulièrement si elles sont entreposées chez le prestataire de service

---

[91] R. BUYYA, J. BROBERG et A. M. GOSCINSKI, préc., note 62, chap. 1, p. 15.
[92] R. HILL, L. HIRSCH, P. LAKE, et S. MOSHIRI, préc., note 70, p. 97.
[93] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 5-1.
[94] *Id*., p. 5-4.
[95] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 5-5.
[96] *Id*.

conjointement à des données de clients différents. Dans un tel cas, le modèle SaaS doit prendre soin de bien définir les frontières par des mesures de sécurité adéquates aux types de données en traitement par les clients[97]. Finalement, la pérennité des données ainsi déposées dans les nuages est également un élément à prendre en considération. Les pratiques de sauvegarde du fournisseur exposent probablement les données à des faiblesses additionnelles compte tenu de la nature même des services infonuagiques, qui est, entre autres, de permettre la transnationalisation des données. Leurs réplications augmentent ainsi les risques de divulgation et d'accès non autorisé[98]. Ces problèmes de nature exogène à l'entreprise peuvent tout de même avoir des répercussions importantes quant à la confidentialité des données. Nous reviendrons sur cette question subséquemment dans ce mémoire[99].

Figure 5. SaaS



[97] *Id.*
[98] N. W. VERMEYS, préc., note 75, p. 203., LCCJTI art 20.
[99] Voir Première partie, 2.3.2 La confidentialité; Seconde Partie 1.3.1 La confidentialité des données des organismes publics; et 2.3.1 L'obligation d'assurer la confidentialité des données.

### 1.4.2 La plateforme sous forme de service (PaaS)

Pour les acquéreurs de service infonuagique recherchant des exigences spécifiques et voulant développer leur propre application, la plateforme sous forme de service est la solution. Selon l'Office québécois de la langue française, le PaaS se définit comme suit : « 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. »[100]. Dans le modèle PaaS, la plateforme et les outils pour les développements système ou d'application sont hébergés et mise à la disposition du client par un fournisseur de service. Habituellement, cette plateforme offrira

> « […] les outils et une infrastructure conventionnelle requis pour le développement d'applications ainsi que des services d'installation de flux de travail pour la conception d'applications, le développement, les tests, le déploiement et l'hébergement, en plus des services d'intégration Web, de base de données, de sécurité, de stockage, de gestion des versions, de communication et de collaboration. »[101] (notre traduction).

Ces outils sont par ailleurs structurés pour supporter une abondance de clients, une grande quantité de données et être accédés depuis n'importe où sur Internet[102].

Le modèle PaaS permet au développeur de se consacrer sur ce qu'il fait de mieux : la programmation et l'utilisation des API[103]. En effet, il n'exercera aucun contrôle et n'aura aucune responsabilité pour l'infrastructure sous-jacente du nuage. Le fournisseur du service aura quant à lui la responsabilité de toutes les opérations et de toute la maintenance requise par la plateforme[104].

En plus des avantages évoqués auparavant, ce modèle comprend les mêmes atouts que le SaaS[105]. Les coûts de maintenance et de distribution seront grandement réduits. L'application

---

[100] OQLF., préc., note 10.
[101] S. MURUGESAN, I. BOJANOVA, préc., note 34, Chap 1., p. 7.
[102] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 6-1.
[103] OQLF., préc., note 10. « API » : « Interface contenant les fonctions nécessaires au développement d'applications. ».
[104] R. HILL, L. HIRSCH, P. LAKE, et S. MOSHIRI, préc., note 70, p. 99.
[105] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 6-3.

pourra évoluer conjointement avec la demande et finalement offrir la possibilité de centraliser les données.

Les inconvénients seront à peu de chose près les mêmes que le modèle d'exploitation commerciale des logiciels en tant que service. Notamment à ce qui a trait aux risques liés à la sécurité des navigateurs qui seront utilisés pour accéder aux plateformes ainsi qu'à la dépendance au bon fonctionnement du réseau Internet[106]. De plus, une importance particulière doit être accordée à la notion de portabilité entre les différentes plateformes infonuagiques[107], y compris lorsque des langages de programmation standard sont employés. En effet, dans de tels cas, la transition d'une plateforme à une autre peut provoquer de grave problème d'interopérabilité. L'utilisation d'interface généralisée aux services de la plateforme peut atténuer l'empreinte du fournisseur de services[108].

Figure 6. PaaS


[106] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 38.
[107] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 6-4.
[108] *Id*., p. 6-4.

### 1.4.3 L'infrastructure sous forme de service (IaaS)

Le plus important engagement possible envers les services infonuagique est sans aucun doute celui de l'infrastructure sous forme de service. Ce mode de fonctionnement représente un accès à une infrastructure informatique virtualisé, permettant à un utilisateur de ce service d'y installer le système d'exploitation de son choix et d'y exécuter les services requis pour son organisation. L'infrastructure en tant que service sera clarifiée pour certains si nous la nommons « matériel sous forme de service ». En effet, plutôt que de se surmener à assembler ses propres fermes de serveurs, un organisme peut décider d'utiliser l'infrastructure offerte par des entreprises professionnelles[109]. Ce modèle offre aussi de grandes libertés aux entreprises, mais est souvent perçu comme une technologie incroyablement perturbatrice. Elle pourrait entre autres, si le besoin se présente, métamorphoser une petite entreprise en grosse compagnie pratiquement du jour au lendemain. Il permettra à cette dernière de bénéficier d'une infrastructure complète, comme s'il avait lui-même mis en place la quincaillerie, mais sans les risques et les coûts reliés à l'exploitation de ces derniers. Le NIST définit l'IaaS comme étant:

> « *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).* »[110].

Essentiellement, un fournisseur de service IaaS crée une structure informatique imposante, et permet à l'utilisateur de créer des ressources virtuelles selon ces besoins. L'administrateur interagit avec le modèle IaaS pour créer des serveurs virtuels, des espaces de stockage virtuels, des réseaux virtuels, et utilise ces systèmes virtualisés pour créer ou compléter sa solution d'affaires informatique[111].

Tel que susmentionné, le client d'un système d'infrastructure sous forme de service aura la possibilité de prendre plusieurs décisions concernant les paramètres des systèmes souhaités.

---

[109] B. FURHT, et A. ESCALANTE, préc., note 73, p. 340.
[110] P. MELL et T. GRANCE, préc., note 27, p. 3.
[111] S. BARRIE, préc., note 74, chap. 4, p. 67.

Chez la plupart des fournisseurs, la taille de la machine virtuelle est définie par le nombre de cœurs[112], la puissance des processeurs[113], la quantité de mémoire vive[114], la taille d'espace de stockage ainsi que les capacités réseau nécessaires, elle sera soit livrée avec des valeurs prédéfinies ou configurables par le client. Leur utilisation est habituellement payable à l'heure[115], mais comme chaque prestataire de service aura différentes ressources avec des politiques de prix distinctes, il n'y a aucune règle commune définissant les types des ressources virtuelles[116]. À titre d'exemple, Microsoft a récemment démontré avec l'hyperconvergence de ses services infonuagiques pouvoir traduire les trois milliards de mots des cinq millions d'articles de Wikipédia en moins d'un dixième de seconde[117]. Voilà, ce qu'on appelle de la puissance à la demande.

Tout comme les autres modèles de prestation de service infonuagique, l'avantage le plus important demeure financier. L'IaaS permettra une réduction des coûts d'acquisition des serveurs et de l'infrastructure réseau générale de l'entreprise. Comme les ressources disponibles peuvent être aisément accrues ou réduites, l'incidence des crêtes impromptues, peu importe si elles sont de nature réseautique, d'espace ou de puissance de calcul, sera limitée en conséquence puisqu'ils ne requerront aucun investissement d'achat ou de maintenance[118].

L'IaaS offre aussi le plus haut niveau de compatibilité avec les systèmes et les applications d'origines liés à l'installation actuelle des utilisateurs potentiels. En effet, tout peut être géré par l'administrateur responsable de l'infrastructure contractée. Donc, aucun besoin de modifier les services ou les logiciels utilisés peu importe leur prérequis, il ne suffit que de les installer.

---

[112] OQLF., préc., note 10, « Cœur » : « Unité de base de traitement de données d'un processeur. ».
[113] *Id*., « Processeur » : « Unité fonctionnelle d'un ordinateur, constituée de circuits électroniques, qui interprète et exécute les instructions. ».
[114] *Id*., « Mémoire vive / RAM » : « Mémoire dans laquelle les données sont accessibles et modifiables de façon courante et qui ne conserve pas son contenu lorsque l'ordinateur est mis hors tension. ».
[115] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 7-1.
[116] S. MURUGESAN, I. BOJANOVA, préc., note 34, Chap 1., p. 447.
[117] Mark HACHMCN, «Microsoft's FPGA-powered supercomputers can translate wikipoedia faster than you can blink », (26 Septembre 2016), PCWorld, en ligne : <https://www.pcworld.com/article/3124486/hardware/microsofts-fpga-powered-supercomputer-can-translate-wikipedia-faster-than-you-can-blink.html>, consulté le 28 avril 2019).
[118] L. BADGER, T. GRANCE, R. PATT-CORNER et J. VOAS, préc., note 66, p. 7-6.

Encore et même plus sous ce modèle, l'accès au réseau ainsi que sa fiabilité aura un effet direct sur la performance du système. En outre, l'ouverture que permet l'IaaS apportera son lot de menaces de sécurité additionnelle. En revanche, ces mêmes aléas pourront être tout aussi présents sur une structure intérieure à l'entreprise, ou dans le cas où l'IaaS servirait d'extension à un environnement local. Malgré les possibilités qu'offre cet environnement, il ne faut pas penser que les interactions inhabituelles avec les systèmes ne seront pas scrutées à la loupe par le prestataire de service, et ce, même si la responsabilité à gérer les mesures de sécurité associées aux machines virtuelles, ainsi qu'au service réseau incombe au locataire.

Autre que le matériel, une mince couche du système, lorsqu'expatrié, restera inaccessible et partiellement inconnue aux gestionnaires de l'Infrastructure louée, il s'agit de l'hyperviseur. Cette mince couche logicielle « supervise l'allocation dynamique des ressources à chacune des machines virtuelles qu'il contribue à créer et à administrer. »[119]. La responsabilité de celle-ci incombe au prestataire de service. Pourtant ce service, loin d'être sans faille et de ne nécessiter aucun entretien, est responsable d'une partie de l'isolation et de la robustesse des ressources virtuelles allouées.

Lorsque l'infrastructure est sur un service public, communautaire ou hybride, l'isolation entre les infrastructures sera essentielle pour proscrire les interactions au sein de celles-ci et ainsi éviter que le prestataire devienne un vecteur de menace lié à l'intégrité et à la disponibilité des données. Nous exposerons ces éléments dans le deuxième chapitre de ce mémoire.

[119] OQLF., préc., note 10, « Hyperviseur ».

***Table 1.2*** *Cloud service models*

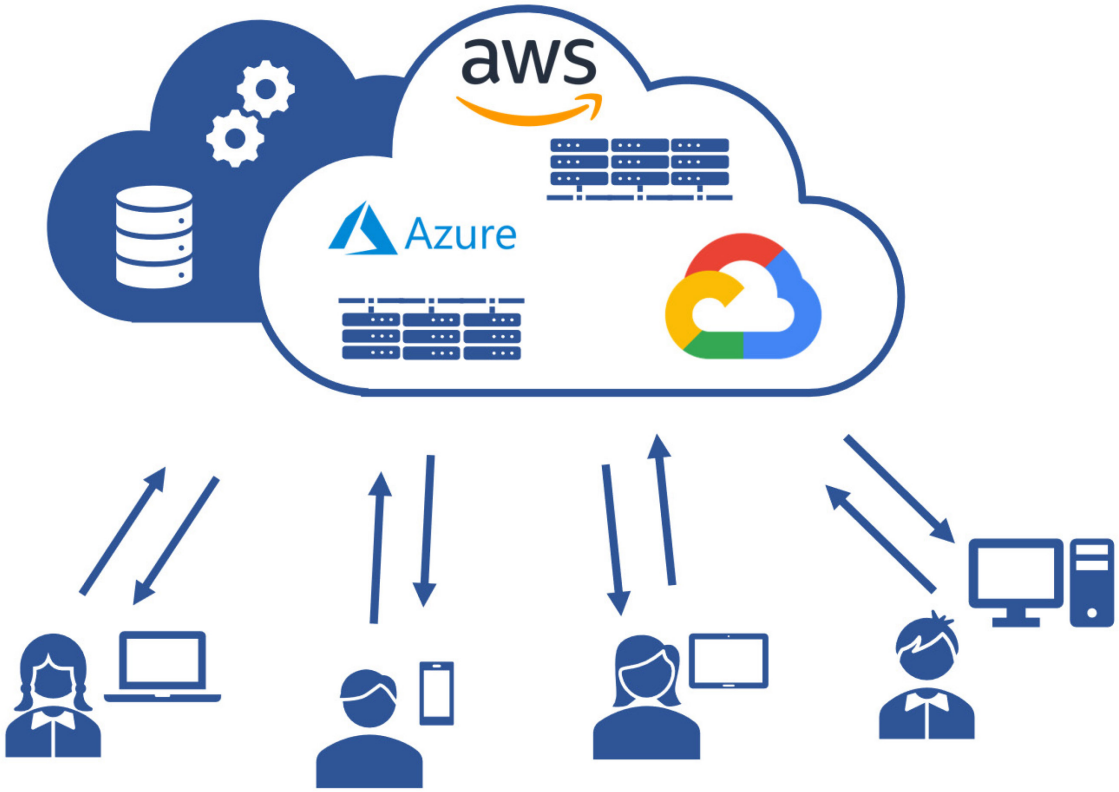
| Service model | Capability offered to the user | Controllability by users |
|---|---|---|
| Software as a service (SaaS) | Use of applications that run on the cloud. | Limited application configuration settings, but no control over underlying cloud infrastructure – network, servers, operating systems, storage, or individual application capabilities. |
| Platform as a service (PaaS) | Deployment of applications on the cloud infrastructure; may use supported programming languages, libraries, services, and tools. | The user has control of deployed applications and their environment settings, but no control of cloud infrastructure – network, servers, operating systems, or storage. |
| Infrastructure as a service (IaaS) | Provisioning of processing, storage, networks, etc.; may deploy and run operating systems, applications, etc. | The user has control of operating systems, storage, and deployed applications running on virtualized resources assigned to the user, but no control over underlying cloud infrastructure. |

Tableau I. Modèle de service infonuagique selon le NIST.

Pour conclure ce chapitre, nous constatons, à la lumière des définitions et des explications ci-dessus, que la conceptualisation des services infonuagiques provient de caractéristique distinctive basée sur différents modèles de déploiement et de services. Certaines de ces transitions sont ou seront inévitables. Ces impartitions de service informatique peuvent certainement faciliter des tâches et pallier certains problèmes, mais ils entraîneront aussi une perte de contrôle sur les données et sur la sécurité de l'information. Pourtant, plusieurs individus et institutions utilisent déjà certains services infonuagiques, quelques-uns d'entre eux consciemment et d'autres sans vraiment être au courant des conséquences liées à leurs utilisations; pensons à Office 365, Google Docs et Dropbox pour ne nommer que ceux-là.

Nous croyons que la dernière catégorie, c'est-à-dire l'IaaS, est la plus prédisposée aux grandes infrastructures informatiques universitaires déjà mises en place puisqu'elle permettra de répondre aux besoins criants des universités de toujours être à la fine pointe de la technologie. Néanmoins, les gestionnaires qui voudront faire le passage à une infrastructure complète ou une partie sur ces systèmes devront se poser de sérieuses questions. C'est, d'autre part, sur cette forme de service que nous concentrerons notre analyse.

Figure 7. IaaS



# Chapitre II : Le cadre sécuritaire propre à l'utilisation de l'IaaS

Afin de bien saisir dans quelles conditions nous pouvons consentir à l'impartition des systèmes informatiques d'une institution universitaire vers une infrastructure infonuagique externe nous devons avant tout connaître les types de données présentes à l'intérieur des universités. Par ailleurs, il sera nécessaire de caractériser ces données selon un degré de classification[120], c'est-à-dire le niveau de sensibilité des différentes informations qu'elles véhiculent[121]. Au même titre que précédemment mentionné, nous ne nous limitons pas au dépôt de données infonuagique dans le cadre de ce mémoire, mais il est fondamental de ne pas perdre de vue que tout ce qui voyage sur les infrastructures informatiques est en soi une donnée[122]. Aussi, comme nous le verrons, les données informatiques se distinguent de l'information en droit. Nous verrons également que les données hébergées à une infrastructure sous forme de service seront forcément liées à une ou plusieurs obligations de sécurité informationnelle issue de la « triade CID »[123] soit, la confidentialité, l'intégrité et la disponibilité des données. Finalement, pour évaluer l'importance et la classification des données universitaire, nous avons choisi d'utiliser la méthode d'analyse de risque puisqu'elle est le vecteur principal de l'obligation de sécurité informationnelle[124]. Qui plus est, selon la doctrine, l'analyse de risque permet d'identifier si l'obligation de moyen est respectée et appliquée de manière raisonnable[125]. Pour répondre au besoin de sécurité informationnelle dans la mesure du raisonnable, le NIST propose quatre étapes[126] :

1. L'identification des risques;
2. L'analyse des risques;

---

[120] OQLF., préc., note 8, « classification » : « Opération qui consiste à grouper formellement des éléments de configuration, des incidents, des problèmes ou des changements, en fonction de leur type. ».
[121] Le niveau de sensibilité (mesures de sécurité propres) auquel nous faisons ici référence est exigé par le législateur à l'article 63.1 de la *Loi sur l'accès*.
[122] OQLF., préc., note 8, « donnée » : « Représentation d'une information, codée dans un format permettant son traitement par ordinateur. ».
[123] N. W. VERMEYS, préc., note 68, p. 24.
[124] *Id*., p. 47.
[125] *Id*., p. 72 – 75; LCCJTI, art. 25.
[126] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*, Guide for Conducting Risk assessments*, SP 800-30 Revision 1, 2012, chapitre 2 page 5, en ligne : <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, (consulté le 28 avril 2019).

3. La réponse aux risques;
4. La surveillance des risques.

L'analyse de risque nous permettra, entre autres, de bien comprendre les valeurs des données touchées ainsi que les répercussions juridiques d'un tel changement de paradigme.

## 2.1 Les types de données présentes dans les universités

Les données issues du milieu universitaire sont considérables, quel que soit le domaine ou les intérêts, ces données changent le visage de notre monde. Elles peuvent permettre de guérir une maladie, être responsables de ces publicités ciblées qui nous embêtent constamment ou encore contenir les identifiants de connexion nous permettant d'accéder à des ressources. Souvent, les données sont confondues comme étant un synonyme d'informations, mais en informatique, il s'agit plutôt d'un hyponyme. Les données se réfèrent aux renseignements qui sont lisibles par la machine plutôt que par l'homme[127,128], une fois colligées ou associées, elles deviennent informations. Dans nos institutions d'enseignement, nous croyons que, par notre expérience ainsi que par notre analyse du recueil des règles de conservation des documents des établissements universitaires québécois, ces données se divisent en cinq grandes familles; celles issues de la recherche (2.1.1), de l'enseignement (2.1.2), de la gestion de l'établissement (2.1.3), ainsi que les données concernant les étudiants (2.1.4) et les données qui touchent les membres du personnel (2.1.5). Bien évidemment, les énumérations des sections suivantes sont loin d'être exhaustives. Ils nous permettront néanmoins de donner un bon aperçu de la diversité ainsi que la pluralité de l'information présente dans nos établissements d'enseignement.

### 2.1.1 Les données de recherche

Les données de recherche sont « issues de l'observation, de l'expérimentation ou dérivées de sources existantes qui sont analysées en vue de produire ou de valider des résultats

---

[127] Carlo BATINI, Monica SCANNAPIECO, *Data and Information Quality, Dimensions, Principles and Techniques*, Switzerland, Springer, 2016, p. x-xi (preface).

[128] Nous incluons dans ces données, les métadonnées. OQLF., préc., note 10, « métadonnées » : « qui sont un « Ensemble structuré de données accompagnant un ouvrage et servant notamment à en décrire le contenu et le format, à assurer son indexation dans les moteurs de recherche et les bases de données, et à faciliter la gestion des droits d'auteur qui y sont liés. ».

de recherche originaux. »[129]. Il est important de préciser que, dans de nombreuses universités canadiennes, les données recueillies dans le cadre de projets de recherche financés par les gouvernements fédéral ou provinciaux sont considérées comme appartenant à l'université[130]. Ce fait n'est tout de même pas généralisé. En effet, comme le précise l'honorable Marie-France Bich : « [l]'œuvre du salarié appartient à l'employeur, mais non l'âme de cette œuvre […] »[131]. Ainsi, les établissements d'enseignement établissent habituellement ces droits dans des contrats individuels ou dans un contrat collectif de travail. Quant aux lois canadiennes, elles n'établissent pas de manière explicite le propriétaire des œuvres issues de la recherche universitaire. L'Université de Montréal stipule trois facteurs extérieurs à prendre en considération afin d'encadrer la gestion des données de recherche :

> « […]
> - Le contrat de travail ou les politiques de votre institution d'attache;
> - Les conventions dans votre domaine concernant le niveau de reconnaissance de votre participation à un projet;
> - L'organisme qui vous finance qui peut s'attribuer conjointement la propriété intellectuelle ou s'accorder une licence sur les données. […]»[132].

Les corpus issus de la recherche peuvent être, au sein des universités, représentés par des publications telles, des livres, des mémoires, des thèses ou même encore des brevets. En plus de ces réalisations, les données de recherches peuvent être aussi sous forme d'enregistrements sonores, de bases de données d'images ou de vidéos. En complément, elles pourraient aussi être engendrées par des chaires industrielles ou gouvernementales, des projets militaires, médicaux ou autres. Dans la majorité de ces cas, elles pourront être soumises à des accords de non-divulgation[133]. Nous devons aussi qualifier de données se rapportant à la recherche toutes formes

---

[129] Bibliothèque, Université de Montréal « Gestion des données de recherche », en ligne : <https://bib.umontreal.ca/gerer-diffuser/gestion-donnees-recherche>, (consulté le 28 avril 2019).

[130] Canadian Association for Graduate Studies, « A Guide to Intellectual Property », en ligne : <http://www.cags.ca/documents/publications/working/Guide_Intellectual_Property.pdf> (consulté le 28 avril 2019).

[131] BICH, M.-F., « Emploi et propriété intellectuelle – médiation sur les droits moraux du salarié », Journal du Barreau du Québec, Volume 31 numéro 20, 1999; voir notamment (pour une analyse complète de la question des « notes de cours » : *Syndicat des professeurs de l'État du Québec (SPEQ)* c *Ministère de l'Agriculture, des Pêcheries et de l'Alimentation du Québec (MAPAQ)-Institut de technologie agroalimentaire (ITA)*, 2018, 33548 (QC SAT).

[132] *Id.*, préc note 129.

[133] OQLF., préc., note 10, « accord de non-divulgation » : « Accord signé entre deux parties afin de protéger des informations qui doivent demeurer confidentielles. ». Souvent, ces Accord de non-divulgation seront entre

de licences ou de technologies réservées et restreintes à certains domaines. Les données de recherches sont souvent associées au « big data »[134]. Ces mégadonnées[135] ont souvent un lien étroit avec l'infonuagique à cause de leur démesure. Ce n'est donc pas une coïncidence si l'essor de ces banques de données massives survient alors que l'infonuagique croît avec importance[136]. La recherche universitaire s'empare de ce créneau[137], nous constaterons dans un avenir rapproché où seront entreposés ces pétaoctets[138] de données[139].

### 2.1.2 Les données d'enseignements

Des données qui concernent l'enseignement sont elles aussi inévitablement présentes au sein des infrastructures universitaires. Des informations de second plan comme les répertoires publics des cours, des séances offertes, des horaires ou des diplômes décernés peuvent s'y retrouver, mais également des travaux scolaires, des dissertations, des rapports de stage, des énoncés de laboratoire, des tableaux de résultats scolaires, ainsi de suite. Ajoutons à ces écrits, toutes les œuvres liées à l'enseignement, incluant, mais sans se limiter aux plans de cours ainsi qu'aux notes de cours. De plus, les établissements d'enseignement sont habituellement liés par une obligation de conserver les évaluations passées pour une période de temps définie dans les politiques et les règlements de l'institution[140] en plus des copies des épreuves scolaires en cours

---

l'université et une ou des entreprises soucieuses de protéger le développement ou les résultats issue d'une recherche, habituellement des conséquences importantes au non respects de ces conditions sont explicitement définis.

[134] Souvent traduit en français par « mégadonnées, données volumineuses, données massives ou données de masse, » OQLF., préc., note 10, « mégadonnées » : « Ensemble des données produites en temps réel et en continu, structurées ou non, et dont la croissance est exponentielle. ».

[135] Nous ne traiterons pas de cette notion spécifique aux fins de ce mémoire, mais cette notions de moissonnage est tout de même inévitablement entreposé sur des systèmes infonuagiques.

[136] S. MURUGESAN et I. BOJANOVA, préc., note 34, p. 551.

[137] Voir notamment « À la conquête du big data : Polytechnique Montréal recrute le scientifique de renom Andrea Lodi », Carrefour de l'actualité, Polytechnique Montréal, mai 2015, en ligne : <http://www.polymtl.ca/carrefour-actualite/nouvelles/la-conquete-du-big-data-polytechnique-montreal-recrute-le-scientifique-de-renom-andrea-lodi>, (consulté le 28 avril 2019).

[138] OQLF., préc., note 10, « pétaoctets » : « Unité de mesure égale à 1 125 899 906 842 624 octets, soit 2 à la puissance 50, souvent arrondie à un million de milliards d'octets, utilisée pour exprimer la capacité de stockage d'une mémoire. ».

[139] S. MURUGESAN et I. BOJANOVA, préc., note 34, p. 541.

[140] Voir notamment « Règlement des études de premier cycle », Université de Montréal, en ligne : <http://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/reglement-des-etudes-de-premier-cycle/>, (consulté le 28 avril 2019).

ou à venir. Toutes ces données pourront être conservées en format papier, dans quel cas elles ne risquent pas d'être subjuguées à un avenir dans les nuages. Toutefois, dans la circonstance où elles seront capturées par numérisation[141] ou d'origine numérique, leur prédisposition à l'infonuagique demeure probable.

### 2.1.3 Les données de gestion

Les données de gestion sont présentes en grandes quantités. Nous les subdivisons en deux grandes familles. Premièrement les données de gestions de l'établissement, telles que les règlements, les états de compte, les relevés de dépenses, les données financières, les listes d'accès aux locaux[142]. En second lieu, la deuxième famille est composée des données liées aux traitements concernant les ressources informationnelles qui sont décrites par Nicolas Vermeys comme incluant :

> « […] les logiciels, ordinateurs, réseaux et infrastructures qui composent les systèmes d'information qui compilent, utilisent communiquent et entreposent celle-ci, mais également toute autre ressource associée au traitement de l'information, ainsi que, il va sans dire, l'information elle-même. »[143].

Bien entendu, dans notre cas, c'est l'information issue des ressources informationnelles qui nous intéresse, tel que les données en lien avec les systèmes d'exploitation[144], les évènements systèmes[145], les informations concernant l'infrastructure informatique[146] de

---

[141] OQLF., préc., note 10, « numérisation » : « Conversion d'informations analogiques (son, image, texte) en valeurs numériques correspondantes, manipulables par ordinateur. ».
[142] CREPUQ, « Recueil des règles de conservation des documents des établissements universitaires québécois (édition électronique à jour le 30 mai 2002) », Montréal, en ligne : <https://www.bci-qc.ca/wp-content/uploads/2017/05/Recueil-regles-conservation-CREPUQ.pdf>, (consulté le 28 avril 2019).
[143] N. W. VERMEYS, préc., note 75, p. 21.
[144] OQLF., préc., note 10, « système d'exploitation » : « Logiciel de base d'un ordinateur chargé de commander l'exécution des programmes. ».
[145] *Id*., « système d'exploitation » : « Événement » de l'anglais « Log » : « Signal qui permet, par ses différents états, d'indiquer la situation ou l'évolution d'une partie d'un système. Tout fait significatif pour un traitement. ».
[146] *Id*., « infrastructure informatique » : « 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. ».

l'institution, les ressources disponibles, les schémas réseaux[147], les règles de coupe-feu[148], et les clés privées[149] et parfois même des mots de passe[150].

### 2.1.4 Les données concernant les étudiants

Naturellement, nous ne pouvons parler d'institution d'enseignement sans faire mention des étudiants y faisant passage. Leur séjour sur les bancs d'école ne se fera pas sans la collecte préalable de quelques renseignements personnels. Mentionnons d'emblée leur prénom[151], nom,[152] adresse électronique[153], adresse[154], ainsi que celles de leurs tuteurs. Également, des informations liées au statut d'étudiant incluant le matricule[155], le code permanent[156], des informations de nature judiciaires[157] et les diplômes octroyés ou en voie de l'être. Nous ne pouvons pas passer outre le fait que nous retrouverons aussi des données bancaires les

---

[147] OQLF., préc., note 10, « schémas réseaux » : « Ensemble d'équipements, par exemple des ordinateurs, reliés par des voies de télécommunications (avec ou sans fil, par ligne spécialisée ou non) ».

[148] *Id*., « coupe-feu » : « Dispositif informatique qui permet le passage sélectif des flux d'informations entre le système informatique de l'entité et un réseau externe, dans le but de neutraliser les tentatives d'accès non autorisé au système en provenance de l'extérieur de l'entité et de maîtriser les accès vers l'extérieur. ».

[149] *Id*, « clé privée » : « Clé cryptographique, composante de la biclé, qui est connue de son unique propriétaire et utilisée par lui seul pour déchiffrer un message dont il est le destinataire, ou pour signer un message dont il est l'expéditeur. ».

[150] *Id*, « mot de passe » : « Authentifiant prenant la forme d'une chaîne de caractères alphanumériques, généralement choisie par l'utilisateur, que celui-ci doit entrer lors de la procédure d'accès à un système informatique, notamment à un réseau ou à sa boîte aux lettres électronique. ».

[151] *Loi sur l'accès à l'information*, art. 19. Cet article mentionne que le nom lorsque celui-ci est mentionné avec d'autres renseignements personnels le concernant ou lorsque la seule divulgation du nom révélerait des renseignements à son sujet.

[152] *Id*.

[153] Pour qu'une adresse électronique soit considéré comme un RP, elle doit permettre d'identifier la personne, indéniablement, la plupart des institutions s'enseignement utilise « prenom.nom@université.ca » comme courriel lorsqu'il est attribué à l'étudiant. Voir notamment : Éloïse GRATTON, *Understanding Personal Information, Managing Privacy Risks,* Markham, LexisNexis, 2013, p. 32; ainsi que Pierre Trudel, France Abran & Gabriel Dupuis*, Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions,* Rapport préparé pour la Direction des politiques du ministère des services gouvernementaux du Québec (Montréal : chaire L.R. Wilson et CRDP, 2007) at 55.

[154] LPRPSP, art. 2.

[155] La Commission d'accès à l'information rappelle qu'en vertu de la *Loi sur l'accès* « les renseignements qui permettent d'identifier une personne sont nominatifs. Lorsque, par exemple, la note est juxtaposée à un nom ou à un numéro de matricule qui commence par l'année d'inscription ou par les trois premières lettres du nom de famille, il s'agit de renseignements nominatifs. »*;* CAI, « LA GESTION DES RENSEIGNEMENTS PERSONNELS DANS LES UNIVERSITÉS ET CÉGEPS », 1995, *en ligne :* <http://www.cai.gouv.qc.ca/documents/CAI_FI_rens_pers_univ-cegep.pdf> (consulté le 28 avril 2019).

[156] *Id*.

[157] Dans cette cause, des conclusions d'enquêtes et des rapports d'enquêtes entre autres étaient conservé au dossier d'une étudiantes : voir *Portal* c. *Institut national de la recherche scientifique* 2018 QCCAI 255.

concernant, de même que leur numéro d'assurance sociale[158]. De plus, dans certains cas, les informations concernant les étudiants non admis, mais ayant tout de même fait préalablement une demande d'inscription à un programme d'études ou à des cours dans un établissement seront parfois conservées.

### 2.1.5 Les données concernant les membres du personnel

Finalement, en complémentarité aux étudiants, nous retrouverons les employés de ces mêmes institutions. Bien entendu, nous retrouverons pour eux essentiellement les mêmes informations que pour les étudiants à savoir le numéro d'assurance sociale[159], leur adresse, numéro de téléphone, la situation familiale, les antécédents professionnels, leur formation, bien entendu certaines informations financières[160], comme le numéro de compte bancaire, de même que des renseignements de nature médicale[161] et d'assurance, les antécédents ou procédure judiciaires en cours[162], voire même le nombre d'heures de navigation sur Internet ou les contenus visités[163].

Toutes ces caractéristiques rendent les identités de ce collectif issu du monde de l'enseignement facilement identifiables et retraçables. Conformément à la nature du rôle des institutions d'enseignements, il pourrait sembler tout à fait conforme de détenir autant de renseignements personnels. Éloïse Gratton mentionne concernant la conservation des dossiers médicaux sur les employés que « *Employers or insurers may wish to access and use the medical or health information of their employees or clients. Medical files are normally kept private; nevertheless, their consultation may become necessary in certain specific situations.* »[164]. *A*

---

[158] LPRPSP, art. 2.
[159] Selon le Règlement sur l'assurance-emploi qui est entré en vigueur le 30 avril 2013, les employés doivent fournir leur NAS à leur employeur, Règlement sur l'assurance-emploi (DORS/96-332).
[160] Éloïse GRATTON, *Understanding Personal Information, Managing Privacy Risks*, Markham, LexisNexis, 2013, p. 394.
[161] *Id*., p. 392; voir également *Université du Québec à Montréal* c. *Mailhot* 2018 QCCQ 2375, dans laquelle des renseignements de nature médicale ont été conservés et transmit à un tiers par une université.
[162] Voir notamment : *L.C.* c. *Syndicat de la fonction publique du Québec*, 2017 QCCAI 309; *S.S.* c. *Commission scolaire de Laval*, 2017 QCCAI 137; ou encore *V.P.* c. *Université A*, 2011 QCCAI 280.
[163] Dans cette cause, un stagiaire en enseignements a été renvoyé de l'université entre autres à la suite de l'utilisation de système informatiques pour le visionnement de site Internet à caractère pornographique. *Addy* c. *Commission scolaire Eastern Township*, 2010 QCCS 1708.
[164] É. GRATTON, préc., note 160, p. 392.

*contrario*, la Commission d'accès à l'information rappelle aux étudiants des universités et des collèges que lors de l'inscription, nul n'est tenu de communiquer son NAS[165]. Nonobstant les questions pouvant porter à l'interprétation à savoir si une université doit ou ne doit pas conserver autant d'information sur les individus la fréquentant, force est de constater que de multiples informations de nature personnelle sont conservées au sein des institutions d'enseignement. Nous traiterons ultérieurement les obligations corollaires à cette conservation.

## 2.2 La classification des données présentes dans les universités

D'un point de vue juridique, ces catégories de données formulées ne sont évidemment pas aussi pertinentes que le niveau de sensibilité des différentes informations qu'ils pourraient renfermer. Le risque est accru selon la sensibilité lorsque les données sont expatriées en dehors des établissements d'enseignement. Il est ainsi essentiel de classer les données institutionnelles en fonction de leur niveau de sensibilité[166] et de leurs valeurs critiques aux universités[167]. Avant toute chose, il est important de mentionner que le législateur impose aux organismes publics l'adoption d'une politique de gestion de leurs documents actifs et semi-actifs[168]. Cette gestion de documents mène inévitablement à la classification de ceux-ci. Elle peut néanmoins avoir plusieurs sens. La classification des documents « est une opération visant à analyser et déterminer le sujet d'un document et à lui attribuer le code de classification et le délai de conservation approprié. »[169]. Cette notion permet, en ce qui nous concerne, d'établir les règles de conservation et de destruction liées à la notion d'intégrité des données, mais sans plus[170].

---

[165] Gouvernement du Canada, « Protéger votre numéro d'assurance sociale », (18 juillet 2018), en ligne : <https://www.canada.ca/fr/emploi-developpement-social/programmes/numero-assurance-sociale/proteger.html>, faisant référence à la décision *Bayle* c. *Université Laval*, 1992, QCCAI 91-05-59.

[166]Notamment pour répondre au requis de l'article 63.1 de la *Loi sur l'accès* que nous verrons ci-après.

[167] Par exemple, le haut niveau de sensibilité d'un rapport rédigé par des professeurs de la faculté de droit de l'Université de Montréal lié à la cause *P.S.* c. *Québec (Ministère du Conseil exécutif)*, 2013 QCCAI 58 dans laquelle il y a le refus de l'organisme de les communiquer dans leur entièreté.

[168] *Loi sur les archives*, L.R.Q., chapitre A-21.l., art. 6.

[169] Cette définition de la classification des documents est issue de l'article 1.4.1 du *Plan de classification uniforme des documents du MSSS*, Santé et Services sociaux, Québec, Février 2011, La classification des documents, quoique requise par la *loi des archives* n'est pas définit par le *plan de classification des documents du ministères de l'Enseignement supérieur, de la Recherche, de la Science et de la Technologie* Version septembre 2013.

[170] CREPUQ, voir préc., note 142.

Nous reviendrons sur ces notions subséquemment. Pour les fins de ce mémoire, la classification de sécurité est celle qui nous intéresse. Elle est définie comme étant :

> « L'attribution d'une mention qui permet de caractériser la valeur et l'importance stratégique d'une donnée détenue par une organisation et, conséquemment, le niveau de protection à lui accorder. »[171].

C'est avec cette valeur que nous pourrons déterminer les contrôles de sécurité appropriés pour la migration de ces infrastructures informatiques (sous forme de données) vers des IaaS.

Nous distinguons quatre niveaux de classification de sécurité de l'information: les données publiques, les données internes/privées, les données confidentielles et les données à accès restreintes[172]. Nous évaluerons ces niveaux en fonction des principes de garanties de sécurité contre les risques tels que l'incidence à l'accès et à la divulgation (notamment par transfert, ou par interception d'un tiers), par leur utilisation, leurs modifications ou la destruction de celles-ci[173]. Malheureusement, il n'existe pas de système quantitatif parfait pour le calcul de la classification d'un élément de données particulier. Conséquemment, d'une université à l'autre, ces classements ainsi que l'importance accordée à chacun de ces éléments peuvent différer. Les listes non exhaustives ne sont utilisées qu'à titre d'illustrations et ne sont pas invariables. Dans d'autres cas, la classification appropriée peut être intrinsèquement évidente, à l'occurrence lorsque l'importance d'une information est ciblée clairement par des lois s'appliquant aux organisations publiques, ou encore par des lois s'appliquant aux entreprises privées. Nous reviendrons dans la deuxième partie de ce mémoire sur ces questions[174].

---

[171] OQLF., préc., note 10, « Classification de sécurité » : « Les mentions varient selon les organisations et les données en cause. La classification de sécurité relative à la confidentialité, par exemple, peut comporter les niveaux suivants: public, diffusion restreinte, confidentiel, secret et très secret. ».

[172] Ces niveaux de classifications sont tirés du *Règlement 117 – Classification et manutention de l'information, Université d'Ottawa*. Malgré qu'il s'agît ici de l'Université d'Ottawa, l'information issue du corpus universitaires québécoises sera sensiblement la même, les niveaux de classification ici mentionnée sont très bien identifié par l'institution., en ligne : <https://www.uottawa.ca/administration-et-gouvernance/reglement-117-classification-manutention-information>.

[173] ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », Éditions OCDE, art. 11, en ligne : <http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm>.

[174] Voir section II, chapitre 1 pour les obligations découlant des lois applicables aux organismes publics et la section II, chapitre 2 pour les obligations découlant des lois spécifiques au secteur privé en lien avec les universités.

### 2.2.1 Les données publiques

Les données devraient être classées comme étant publiques lorsque la divulgation, la modification ou la destruction non autorisée de ces données aurait des conséquences négligeables ou aucun risque pour l'université et ses filiales. Les données publiques peuvent tirer leur origine des cinq types de données précédemment énumérés. Citons pour exemples : les communiqués de presse, l'information sur les cours, les publications de recherche, le répertoire public et les sites Internet publics de l'institution. Bien que les contrôles nécessaires soient négligeables ou inexistants dans le but de protéger la confidentialité des données publiques, un certain niveau de contrôle demeure essentiel pour contrecarrer toutes modifications ou destruction non autorisées de données publiques. Il est important de souligner que comme le mentionne l'article 55 de la *Loi sur l'accès*, « Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas soumis aux règles de protection des renseignements personnels… »[175]. Notons entre autres comme exemple, tel qu'issue de la loi

> « […] 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; »[176].

Bien entendu, puisque les données à caractère public, qui ne sont pas en lien avec des renseignements personnels, sont publiques par définition. Rien dans la loi n'obligera leurs protections, et pourrons sans crainte être diffusé, accessible et puis traités comme bon le semble par l'université. Incluant bien entendu une impartition vers des systèmes infonuagiques externes à l'établissement.

### 2.2.2 Les données internes/privées

Pour ce qui a trait aux données internes et privées à l'établissement, elles devraient être classées ainsi lorsque la divulgation, la modification ou la destruction non autorisée de ces données pourrait entraîner un niveau de risque modéré pour l'université ou ses filiales. À moins d'un avis contraire, toutes les données institutionnelles qui ne sont pas explicitement classées

[175] *Loi sur l'accès,* art. 55.
[176] *Id*., art 57.

sous forme de données confidentielles, restreintes ou publiques doivent être traitées au même titre que des données privées[177]. Nous pouvons qualifier ces données comme étant habituellement destinées à être communiquées uniquement sur la base de la nécessité, soit lorsque l'information doit être connue par un groupe d'individus. Évidemment, un niveau raisonnable de contrôles de sécurité devrait être appliqué à ces données. En outre, les données internes et privées sont de notre point de vue intermédiaire, elles ne sont ni publiques ni confidentielles. Certains auteurs tels que Pierre Trudel croient que la mesure dans laquelle une situation est publique ou privée variera selon le contexte et la circonstance[178]. Nous croyons également que ce principe s'applique aux données internes et privées des établissements d'enseignement. À l'instar des données publiques, les données privées peuvent provenir des cinq types d'informations présentes dans les universités. Nommons pour exemples : les procédures internes et guides opérationnels, l'information comptable et financières, les bons de commande, les ressources électroniques avec abonnement[179], certaines licences et certains logiciels, les indicateurs et statistiques des admissions, des travaux ou encore des copies d'examens[180]. Les informations concernant le personnel académique et les étudiants pourraient, dans certains cas[181], être classées comme étant confidentielles, telles que les numéros d'étudiant et d'employés, mais nous croyons que ces informations si elles ne sont pas inhérentes à d'autres

[177]University of California, Berkeley, «Data classification standard», 16 juillet 2012 (Administrative revision: April 22, 2013) en ligne : <https://security.berkeley.edu/data-classification-standard>, (consulté le 28 avril 2019).

[178] Pierre TRUDEL, « Privacy Protection on the Internet: Risk Management and Networked Normativity» dans Serge Gutwirth *et al*., eds, *Reinventing Data Protection? (Dordrecht, London: Springer, 2009) 317 à 318-319. :*

> « *In order to establish protection that balances all basic rights, we have to take into account the fact that public and private situation lie along a continuum. In cyberspace, nothing is purely public or strickly private, just as nothing is completely black or white. The degree to which a situation is public or private varies according to the context and circumstances.* ».

[179] Habituellement accessible à l'interne par le biais des bibliothèques ou du réseau de l'université.

[180] Dans le jugement *Desvignes* c. *Université du Québec à Montréal*, 2017 QCTAT 243; Il est mentionné que « La professeure explique qu'au moment où elle a remis les copies à la travailleuse, elle a présumé que celle-ci les apporterait à son domicile, car elles s'étaient entendues sur la correction à domicile pour préserver la confidentialité et la sécurité des copies d'examen. ». Bien que ce jugement soit un cas d'accident de travail, il a été démontré clairement le requis de conserver le niveau raisonnable de contrôle requis à des copies d'examens.

[181] Comme par exemple, si le numéro est formé partiellement de la date de naissance. Voir notamment *Dion-Viens* c. *Université Laval*, 2008 QCCQ 640 par 22.

informations personnelles ne constituent pas un risque très important si elles sont portées à la connaissance d'un certain public interne à l'université[182].

### 2.2.3 Les données confidentielles

Dans une perspective plus primordiale, nous retrouvons des données devant être classées comme étant confidentielles. Corollairement, la divulgation, la modification ou la destruction de celles-ci pourraient entraîner un niveau de risque important pour l'université ou ses filiales, mais également pour les individus lorsque ces données confidentielles sont des renseignements personnels[183]. Cette classification doit s'appliquer même en l'absence de loi qui l'exige [184]. L'information confidentielle comprend notamment toute donnée protégée par une entente de non-divulgation, l'information commercialement sensible, y compris les transactions financières connexes, certains renseignements concernant le personnel académique et les étudiants (passé, existant ou futur) tels que Nom, prénom, numéro de téléphone, les numéros de permis de conduire, les numéros de compte bancaire, ainsi de suite. Cette liste partielle est bien entendu encadrée entre autres par l'article 54 de *la Loi sur l'accès* qui confère un caractère confidentiel aux renseignements personnels qui concernent une personne physique et permettent de l'identifier[185].

### 2.2.4 Les données à accès restreint

La classification des données à accès restreinte est la plus névralgique présente dans les universités. L'accès à ces données se doit d'être rigoureusement contrôlé puisque la divulgation et la modification non autorisée ainsi que l'inaccessibilité de ces données auraient de graves répercussions et pourraient entraîner un risque très important pour les employés, les étudiants, les partenaires de l'université et bien entendu sur elle-même. Certains renseignements personnels d'une grande importance ne font pas abstraction à cette catégorie. C'est notamment le cas du Numéro d'assurance social et ses informations concernant les cartes de paiement. En

---

[182] Cette affirmation est basée sur le fait que bien souvent, ces numéros d'identifications sont utilisés pour communiquer, entre autres, les résultats scolaires des étudiants sur des zones internes des établissements.
[183] LCCJTI, art. 20. Dans laquelle une distinction est faite entre les deux concepts.
[184] *Id.* préc., note 172.
[185] *Loi sur l'accès, art.* 54 : « Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier. ».

plus de ces informations relatives à la personne, plusieurs informations issues des TI pourront créer des risques considérables si elles ne sont pas mises en sécurité adéquatement. Ces informations ne sont pas négligeables dans le contexte d'une impartition d'infrastructure informatique vers des systèmes infonuagiques. Notons ici par exemple les consoles centrales de management[186], les sauvegardes de ces éléments et les « credential store »[187] pouvant contenir les éléments suivants : les clés de chiffrements, les mots de passe, ainsi que les certificats électroniques[188]. Finalement, certaines données encadrées par des ordonnances de non-divulgation, malgré que plusieurs d'entre elles seront classifiées comme étant des données confidentielles, pourront avoir un effet très important advenant la violation des clauses de leurs contrats. Effectivement, certaines dispositions contractuelles, sous forme de Condition d'utilisation « *EULA* »[189], peuvent parfois avoir des incidences, souvent monétaires, de plusieurs milliers de dollars. Prenons pour exemples certaines clauses pour abus d'utilisation inadéquate de logiciel[190].

La classification des données institutionnelles, dans un contexte de sécurité de l'information, se doit d'être périodiquement réévaluée, et ce, dans le but de s'assurer qu'elle est toujours au diapason avec les modifications apportées aux obligations légales et contractuelles. Elle devra également faire l'objet d'un réajustement en fonction des changements dans l'utilisation de ces données ou de leur valeur du point de vue de l'université ou de l'un de ses

---

[186] « *Central management console* » - Fournit une interface intuitive et complète pour la gestion, le contrôle et la configuration des déploiements. Grâce à la prise en charge intégrée des bases de données de sécurité et au contrôle d'accès sécurisé granulaire au niveau objet, la console propose aux administrateurs des outils leur permettant de déployer pratiquement tous les projets d'infrastructure en TI.

[187] Nous traduisons « *Credential store* » par un « gestionnaire d'identification ». Il s'agit d'une bibliothèque de données de sécurité, elle peut contenir des certificats de clé publique, une combinaison de nom d'utilisateur et mot de passe ou des billets attestant le droit d'entrer sur un accès ou un service réseau.

[188] Un Certificat électronique est défini selon Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Thémis, Montréal, 1997, p. 19-30 comme étant « un document électronique dont l'objet est d'établir un lien entre une personne et une paire de clés asymétriques. Le certificat contient ainsi différentes informations relatives à l'identité d'un signataire, dont principalement la clé publique de celui-ci. Il est réalisé et signé par l'autorité de certification à l'aide de la cryptographie asymétrique et est, par le fait même, protégé contre les altérations. Il peut être émis, à demande, à tout signataire enregistré auprès d'une autorité de certification. ».

[189] OQLF., préc., note 10, « EULA » : « est un contrat légal entre l'auteur d'une application et l'utilisateur de celle-ci. ».

[190] Le EULA de la compagnie MICIAN pour le logiciel µWave Wizard stipule: *«…Institute undertakes to pay 30.000,00 Euro to MICIAN for any time of use of the software for other purposes as Institute is entitled to by the license agreement for the software… ».*

intervenants. Cette évaluation devrait être effectuée en fonction des rôles et des responsabilités conférés aux différents intervenants en matière de Sécurité de l'information généralement composée par le Secrétaire général, la direction des TI, la direction de la gestion des documents et des archives de l'établissement ainsi qu'un coordonnateur de la sécurité des TI[191]. Advenant que l'un des intervenants ou le gestionnaire de l'infrastructure détermine que la classification d'un certain ensemble de données a changé ou que des lacunes sont présentes dans les contrôles de sécurité existants, des corrections devraient être apportées en temps opportun, proportionnellement au niveau de risque présenté par ces insuffisances.

## 2.3 L'obligation de sécurité

Tel qu'indiqué préalablement, l'objectif de l'obligation de sécurité de l'information est de protéger la disponibilité, l'intégrité et la confidentialité des données institutionnelle[192]. La classification permet évidemment d'évaluer le niveau d'incidence sur les données sommairement, mais ces trois éléments de la triade CID reposent avant toutes choses sur des questions de gestion des risques[193]. Avant de recourir à des IaaS, les universités se doivent de faire une rétrospection sur l'importance de leurs données. Elles sont primordiales pour les universités, et d'autant plus pour les unités de recherche scientifique qui en vivent. Il est nécessaire, par ailleurs, de réitérer l'importance de la gestion des risques informationnels et de s'assurer de mettre déjà en pratique les règles de gouvernance des technologies de l'information. Il incombe aux universités voulant utiliser des services infonuagiques, d'identifier, d'évaluer et de réduire à un niveau acceptable les risques auxquels elles pourraient se heurter[194], et ce, que l'infrastructure de l'établissement soit localement administrée ou que partiellement, voire même

---

[191] Université de Montréal, Secrétariat général, « Directive concernant le stockage de l'information institutionnelle en infonuagique » Numéro 10.54, 6 Juillet 2017, Recueil Officiel, en ligne : <https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/administration/adm10_54-Directive_concernant_stockage_information_institutionnelle_infonuagique.pdf>, (consulté le 28 avril 2019).

[192] « Availability, integrity and confidentiality » voir notamment, Susan HANSCHE *et al*., *Official (ISC)² Guide to CISSP Exam,* Boca Raton, Auerbach, 2004, p.3; Joël HUBIN et Yves POULLET, *La sécurité informatique, entre technique et droit*, Namur C.R.I.D., 1998, p.7.

[193] N. W. VERMEYS, préc., note 75, p.88.

[194] Todd FITZGERALD *et al*., «Information Security and Risk Management », dans Harold F. TIPFON et Kevin HENRY, *Official (ISC)² Guide to CISSP CBK*, Boca Raton, Auerbach, 2007, p.55.

entièrement entreposée dans les nuages de tiers. D'autre part, pour bien saisir leur portée, nous avons analysé ces risques informationnels en annexe[195].

### 2.3.1 La gestion des risques des Infrastructures sous forme de service

La gestion des risques informationnels est définie comme l'« [e]nsemble des activités qui consistent à recenser les risques auxquels l'entité est exposée, puis à définir et à mettre en place les mesures préventives appropriées en vue de supprimer ou d'atténuer les conséquences d'un risque couru. »[196]. Cet exercice peut s'illustrer facilement à l'aide de la figure suivante[197] :

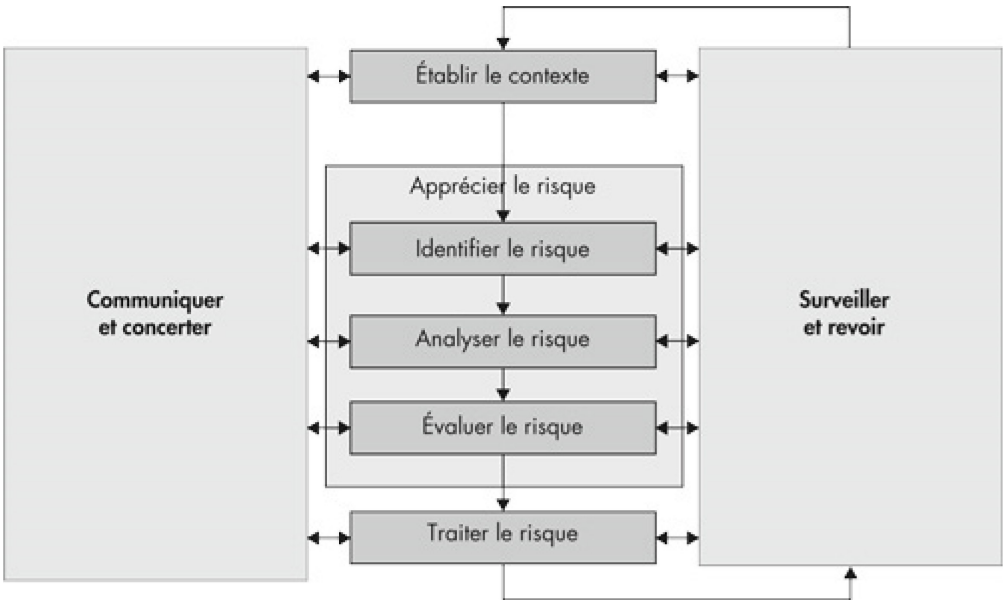



Figure 8. Relations entre les principes de gestion des risques

Malgré la portée juridique du présent mémoire, nous ne pouvons passer sous silence certains risques de nature organisationnels ou techniques. D'autant plus que nous verrons que ces derniers auront des origines ou des incidences normatives, réglementaires et donc juridiques.

---

[195] Voir Annexe 1 : Analyse de Risque.
[196] OQLF., préc., note 10, « gestion du risque ».
[197] Norme ISO/IEC 31000 :2018, « Management du risque », Organisation Internationale de Normalisation (ISO), Genève, 2018.

Il y a autant de systèmes de classification des risques que d'auteurs. Pour les fins du présent mémoire, nous avons choisi de regrouper alors les risques en trois catégories distinctes[198] :

- Les risques organisationnels
- Les risques techniques
- Les risques légaux

Évidemment, ces éléments de risque liés à l'utilisation de l'infrastructure sous forme de service devraient être comparés à ceux inhérents du statu quo, c'est-à-dire de demeurer avec les solutions traditionnelles[199]. Par le fait même, nous observons indubitablement des récurrences entre les risques attribuables à chacun des éléments de la triade CID, puisque certaines menaces peuvent affecter, à plusieurs niveaux, les obligations de sécurité de l'information. Pour bien comprendre la probabilité d'un scénario d'incident, nous utilisons la matrice de la norme ISO 27005:2008 suivante[200] :

Tableau II. Indices de niveau de risque (Probabilité vs Gravité)

| | Probabilité d'incident | Très faible (très rare) | Faible (peu probable) | Moyen (Possible) | Élevé (Probable) | Très élevé (fréquent) |
|---|---|---|---|---|---|---|
| Gravité sur l'université | Très faible | 0 | 1 | 2 | 3 | 4 |
| | Faible | 1 | 2 | 3 | 4 | 5 |
| | Moyen | 2 | 3 | 4 | 5 | 6 |
| | Élevé | 3 | 4 | 5 | 6 | 7 |
| | Très élevé | 4 | 5 | 6 | 7 | 8 |

Elle permet entre autres d'établir le niveau de risque encouru :

- Risque Faible : 0-2

[198] Ces catégories de risques sont tirées de : Roger MILLER et Joanne CASTONGUAY, « rapport de projet sur : La gouvernance des grands projets d'infrastructure publique, La gestion des risques », Montréal, Mai 2006 en ligne : <https://cirano.qc.ca/files/publications/2006RP-17.pdf>, (consulté le 28 avril 2019).
[199] Par solutions traditionnelles, nous sous-entendons un réseau informatique local avec des services locaux, et où la quincaillerie informatique serait entièrement sous le contrôle des administrateurs des universités.
[200] Norme ISO/IEC 27005 :2008, « Technologies de l'information -- Techniques de sécurité -- Gestion des risques en sécurité de l'information », Organisation Internationale de Normalisation (ISO), Genève, 2008, p. 50, Tableau E.1 b).

- Risque Moyen : 3-5
- Risque Élevé : 6-8

La liste des risques principaux que nous avons identifiés[201] pouvant affecter les infrastructures sous forme de service est déconcertante. Évidemment, les stratégies de réponses aux risques dans un contexte d'adoption de l'IaaS devront être d'éliminer, de transférer, d'atténuer ou d'accepter ces risques, mais ils devront également répondre aux obligations de sécurité fixées par les lois et les règlements en vigueur[202]. Voici certains des défis que devront anticiper les universités.

Les risques organisationnels, techniques et juridiques suivants sont issus de différentes sources[203]. Ils ont été choisis puisqu'ils ont été identifiés comme étant les plus névralgiques par les autorités compétentes et pertinentes dans les circonstances[204]. Une analyse de risque sommaire ainsi qu'une explication de chacun de ces risques sont disponibles en annexe[205].

**Les risques organisationnels**

- R.1 : Fermeture ou changement du service infonuagiques[206]
- R.2 : Vendor-Lock-In
- R.3 : Perte de gouvernance (Continuité des activités et résilience)
- R.4 : Défaillance d'un des acteurs liés au service infonuagique[207]
- R.5 : Perte de conformité
- R.6 : Perte de disponibilité due aux activités des colocataires des services infonuagiques.

**Les risques techniques**

- R.7 Panne matérielle liée au réseau
- R.8 Épuisement des ressources (sous provisionnement)

---

[201] Ces risques identifiés sont basés sur les données du *Cloud Security Alliance*, sur les données du European Network and Information Security Agency, ainsi que sur l'expérience de l'auteur des technologies de l'information.
[202] R. MILLER et J. CASTONGUAY, préc., note 198.
[203] ENISA, « Cloud Computing, Benefits, risks and recommendations for information security », Novembre 2009; Sailesh GADIA, « Cloud Computing Risk Assessment, A Case Study», *ISACA Journal*, Volume 4, 2011; Jesus LUNA, D3.2 Risk-Based Decision Making Mechanisms For Cloud Service In The Public Sector, 31 Juillet 2017, en ligne : <https://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Risk-based-decision-making-mechanisms-for-cloud-services.pdf>, (Consulté le 28 avril 2019).
[204] *Id*.
[205] Voir Annexe 1 : Analyse de Risque.
[206] D. P. WHELAN, préc., note 259 p. 25; voir également *Oracle Canada* c. *Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île de Montréal*, 2018 QCCA 10.
[207] *Loi sur l'accès*, art. 70.1.

- R.9 Échec d'isolement
- R.10 Abus malveillants de provenance interne – abu de privilèges
- R.11 Piratage de compte ou de services (y compris l'interface de gestion)
- R.12 Déni de services distribués (DDoS)
- R.13 Vulnérabilités logiciels
- R.14 La perte ou vol de sauvegarde
- R.15 La perte, la divulgation ou la corruption des clés de chiffrement[208]
- R.16 Escalade des privilèges
- R.17 Les attaques d'ingénierie sociale
- R.18 Interception des données en transit
- R.19 Suppression non sécuritaire ou inefficace des données
- R.20 La perte, la compromission ou l'inexistence des « journaux »[209] d'opération et de sécurité
- R.21 Catastrophes naturelles[210]
- R.22 Accès non autorisé/vol d'équipement (accès physiques aux installations)
- R.23 Erreur humaine (interne ou externe)

**Les risques légaux**

- R.25 Confiscation d'équipement par les autorités légales pour criminalistique
- R.26 Risque de changement de juridiction[211]
- R.27 Risque lié aux licences
- R.28 Risque d'obligation de sécurité

[208] Aucune exigence à cet effet a été formulée par les tribunaux, mais une analogie peut être fait avec l'obligation à protéger le NIP d'une carte de débit, voir à cet effet : *Daméus* c. *Banque royale du Canada*, 2004 CanLII 20573 (QC CQ) Cette cause cite plusieurs autres jurisprudences à cet effet.
[209] OQLF., préc., note 10, « journal (informatique) » : « Fichier contenant les données historiques de l'exploitation d'un système sur une période donnée qui est constitué à des fins de sécurité informatique. ».
[210] Le risque de catastrophes naturelles est encadré par la *Loi sur la sécurité civile* (L.R.Q., c. S-2.3). L'article 5 dispose que « Toute personne doit faire preuve de prévoyance et de prudence à l'égard des risques de sinistre majeur ou mineur qui sont présents dans son environnement et qui lui sont connus. ». L'article 6 quant à lui, prévoit que « Toute personne qui s'installe en un lieu où l'occupation du sol est notoirement soumise à des contraintes particulières en raison de la présence d'un risque de sinistre majeur ou mineur, sans respecter ces contraintes, est présumée en accepter le risque. […] ».
[211] *Loi sur l'accès*, art. 70.1.

### 2.3.2 La confidentialité

La principale préoccupation des universités concernant l'infonuagique est de loin la confidentialité de leurs données. En effet, comme nous l'avons souligné précédemment, les infrastructures informatiques des universités sont aux prises avec de nombreux documents ayant une classification de « données confidentielles » ou de « données à accès restreints ». La confidentialité est décrite par l'Office québécois de la langue française comme la « Propriété d'une information ou de renseignements personnels qui ne doivent pas être divulgués à des personnes ou à des entités non autorisées »[212]. Elle sera bien évidemment mise à l'épreuve lors d'une migration complète ou partielle d'une infrastructure conventionnelle vers une infrastructure sous forme de service.

Au Québec, les universités devront se conformer à l'article 25 de la LCCJTI, qui invoque une obligation de moyen[213] à l'effet que :

> « La 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 autorisée de prendre connaissance du renseignement […]. »[214].

Qui plus est, comme le passage à l'IaaS constitue le fait de confier des documents technologiques à un prestataire de service, l'article 26 du même texte législatif trouvera également application :

> « Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'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.
>
> Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité […]. Il doit de même assurer le respect de toute autre obligation

[212] OQLF., préc., note 10, « Confidentialité ».
[213] N. W. VERMEYS, préc., note 75, p.103.
[214] LCCJTI, art. 25.

prévue par la loi relativement à la conservation du document. » (nos soulignements)[215].

Cet article de loi effectue un rappel efficace quant aux obligations de sécurité découlant de l'utilisation d'un IaaS ou de tout autre service infonuagique. Il faut par contre réitérer le fait que « cette obligation ne libère pas la personne responsable de l'accès de sa propre obligation d'assurer la confidentialité des données […]. »[216]. Ainsi, semblablement à ce qu'énoncent les auteurs dans l'« Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », dans le cas où le tiers hébergeur néglige la mise en place des mesures coercitives prévues par la loi, l'université sera, au final, la grande responsable du manquement à l'obligation de sécurité. De plus, il est important de renchérir sur le fait que l'article 26 impose clairement une obligation de résultat[217] en ce qui a trait à la mise en place des moyens technologiques requis pour en assurer la sécurité.

Il importe de mentionner que la loi signale des « […] 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 autorisée de prendre connaissance du renseignement […] »[218](nos soulignements). Sagement, le législateur ne prend des décisions disculpatoires, c'est-à-dire qu'il n'impose pas l'utilisation d'une technologie au détriment d'une autre.

Ainsi, les universités devront identifier ces mesures à adopter en se basant sur un ensemble éclectique de facteurs et de normes. Par exemple, l'ISO a publié, en 2014, la première édition d'un « Code de bonnes pratiques pour la protection des informations personnelles identifiables dans l'informatique en nuage public agissant comme processeur de PII »[219] (nos soulignements). L'année suivante cette norme sera complétée par le « Code de pratique pour les

---

[215] LCCJTI, art. 26.
[216] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 108.
[217] N. W. VERMEYS, préc., note 75, p.103.
[218] LCCJTI, art 25.
[219] Norme ISO/IEC 27018:2014, « Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII », Organisation Internationale de Normalisation (ISO), Genève. Dans laquelle les Renseignements personnel sont identifiés comme étant des « informations personnelles identifiables » ou de l'anglais PII pour « *Personally Identifiable Information* ».

contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage »[220].

Les normes ISO 27017[221] et 27018[222] énoncent certains des principes sécuritaires à prendre en compte dans un environnement infonuagique comme la gestion des actifs, les contrôles d'accès et le contrôle par la cryptographie[223] afin d'assurer la confidentialité des données[224]. Ces contrôles de sécurité sont tirés d'une norme homonyme[225] qui se veut être un texte spécifiant le code de bonne pratique pour le management de la sécurité de l'information. Un des objectifs de ces normes est de veiller à la confidentialité des données en suggérant des mesures d'atténuation efficaces, dont le chiffrement[226].

Toujours en lien avec le chiffrement, notons que l'article 63.1 de la *Loi sur l'accès* mentionne que :

> « Un organisme public doit 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. »[227] (nos soulignements).

Peut-on qualifier le chiffrement des données comme une mesure raisonnable ? Cela dépendra du contexte. Les universités, comme nous l'avons suggéré préalablement, devront sans aucun doute effectuer une évaluation des risques dans le but d'identifier les niveaux de protection requis pour les différents types de fichiers ainsi hébergés sur l'infrastructure en nuage.

---

[220] Norme ISO/IEC 27017:2015, « Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage », Organisation Internationale de Normalisation (ISO), Genève.
[221] Norme ISO/IEC 27017:2015, préc., note 220.
[222] Norme ISO/IEC 27018:2014, préc., note 219.
[223] OQLF., préc., note 10, « Cryptographie » : « Ensemble des techniques recourant à des combinaisons d'algorithmes et de valeurs secrètes, appelées clés, utilisées à des fins de contrôle dans des procédures comme le chiffrement, l'authentification, la non-répudiation et la signature électronique. ».
[224] Claude BAUDOIN *et al*., Cloud Standards Customer council, «Cloud Security Standards: What to Except & What to Negociate, Version 2.0» Août 2016, p. 16.
[225] Norme ISO/IEC 27002:2013 « Information technology – Security techniques – Code of pratice for information security controls », Organisation Internationale de Normalisation (ISO), Genève.
[226] *Id*., p. 28., en effet il y est précisé que l'un des objectifs visés est « *To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and /or integrity of information* ».
[227] *Loi sur l'accès*, art. 63.1.

Mais, somme toute, nous croyons que le besoin de chiffrement est bel et bien fondé. Nous ne sommes d'ailleurs pas les seuls à penser ainsi[228].

Mentionnons toutefois que, malgré la nécessité et l'efficacité du chiffrement des données entreposées sur les dépôts de données infonuagiques, les capacités de traitement dans une infrastructure demeurent limitées. Il existe des recherches sur le traitement de données chiffrées, mais tel que nous l'avons laissé entendre en section précédente, ces développements sont encore au point embryonnaire[229] puisqu'ils ne permettent que certaines fonctions mathématiques[230] et ne pourront vraisemblablement pas être utilisés à court terme pour pallier le problème de confidentialité des données soumises aux infrastructures sous forme de service. Malgré que l'infrastructure en nuage implique la mise en place de systèmes complets sous forme de machines virtuelles et que ces machines puissent utiliser des moyens de cryptages éprouvés[231], il n'en demeure pas moins que la clé de chiffrement sera inscrite en mémoire vive[232] afin de permettre l'utilisation de ces serveurs. En dépit que plusieurs organismes de normalisations recommandent l'utilisation d'un service ou d'un serveur différent pour l'entreposage des clés de chiffrement[233], ces dernières pourront tout de même être connues des fournisseurs de l'infrastructure. Une autre alternative pourrait être l'utilisation de « Secure Tamper-Proof Hardware »[234]. Cette technique détiendrait la fonction d'une boite noire dans laquelle les

---

[228] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p.131.

[229] Gilad-Bachrach, RAN, Nathan DOWLIN, Kim LAINE, Kristin LAUTER, Michael NAEHRIG, and John WERNSING. « Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. » In *International Conference on Machine Learning*, 2016, p. 9, en ligne <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/CryptonetsTechReport.pdf>, (consulté le 28 avril 2019).

[230] Ayub HUSSAIN MONDAL, Manish RANJAN, Monjul SAIKIA, « A Brief Overview of Homomorphic Cryptosystem and Their Applications », *International Journal of Computer Applications* (0975 – 8887) - NCIT 2015, September 2015, en ligne : < https://www.researchgate.net/publication/282783441_A_Brief_Overview_of_Homomorphic_Cryptosystem_and_Their_Applications>, (consulté le 28 avril 2019).

[231] M. BALDWIN, «Azure Disk Encryption for Windows and Linux IaaS VMs», Microsoft Corporation, 15 mars 2019, en ligne : <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption>, (consulté le 28 avril 2019).

[232] OQLF., préc., note 10, « mémoire vive » : « Mémoire primaire d'un ordinateur, rapidement accessible, dans laquelle les données peuvent être lues, écrites ou effacées. ».

[233] CLOUD SECURITY ALLIANCE «SecaaS Implementation Guidance, Category 8: Encryption», Septembre 2012, p. 10, en ligne : <https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf>, (consulté le 28 avril 2019).

[234] Amit SAHAI, « Computing on Encrypted Data » (2008), *International Conference on Information Systems Security,* p. 148-153.

opérations auraient lieu sans que le titulaire de l'équipement ne puisse constater ce qui s'y passe. Encore une fois, ces approfondissements ne sont qu'à leur début[235].

En ce qui concerne les risques énumérés précédemment, plusieurs auront à l'évidence des répercussions importantes sur la confidentialité des données hébergées sur des IaaS. Nous avons soulevé au préalable dans cette section la question de chiffrements, toutefois la gestion des clés est une tâche fastidieuse qui se doit d'être rigoureusement conduite pour éviter la perte, la divulgation ou la corruption des clés de chiffrement (R.15[236]) des systèmes hébergés sous une IaaS.

Regrettablement, les risques sécuritaires liés aux piratages (R.11), aux vulnérabilités logicielles (R.13), aux erreurs humaines (R.16, R.23), ainsi qu'aux attaques externes (R.17) ou internes (R.22) aux services infonuagiques sont difficilement contrôlables. Pour se prémunir de ces risques, les bonnes pratiques ainsi que la conservation de ressources fonctionnelles à l'interne de l'université devraient être préconisées.

Quant aux questions liées à l'emplacement des données (R.26), c'est indubitablement l'article 70.1 de la *Loi sur l'accès* qui est d'intérêt. Il dispose 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. »[237] (nos soulignements).

Comme le mentionnent Raymond Doray et François Charrette, « [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 »[238].

---

[235] Curt CULLENS *et al*., « Always Encrypted with Secure Enclaves », Microsoft Corporation, SQL Docs, 23 Septembre 2018; Microsoft a développé récemment des « *Always-Encrypted Enclave* » dans lequel certains traitements d'informations peuvent être toujours chiffrés.
[236] Se référer aux risques (R.) énumérées à la section 2.3.1 : La gestion des risques des Infrastructures sous forme de service.
[237] *Loi sur l'accès, art. 70.1*.
[238] Raymond DORAY et François CHARETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Yvon Blais, 2001, p. III/70.1-2.

Inversement, si une compagnie s'accorde des droits supplémentaires sur nos données[239], qu'elle est aux prises avec une emprise gouvernementale très stricte, ou que des changements de localisation de service infonuagique surviennent (R.1), l'article 70.1 pourrait alors être transgressé. D'autres risques déjà énumérés pourraient aussi créer un précédent dans ce sens, notamment les risques R.10, R.16 & R.25.

Tout compte fait, nous croyons que l'obligation de confidentialité tacite de l'article 70.1 pose une contrainte à « procéder à un examen détaillé de l'encadrement juridique du territoire visé afin de déterminer si les lois applicables prévoient une protection équivalente »[240].

### 2.3.3 L'intégrité

Dans tous systèmes d'information, les données doivent être protégées lors de l'entreposage, mais également, et d'autant plus lors de leur traitement et de leur transit s'ils véhiculent vers des IaaS. Il s'agit ici de la notion d'intégrité. Elle est définie comme 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. »[241].

Législativement, le concept est défini par 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. […] »[242].

---

[239] Notons ici que Google a annoncé en juin 2017 qu'il cesserons de « lire » nos courriels pour faire de la publicité ciblé. Voir notamment : Mark BERGEN, « Google Will Stop Reading Your Emails for Gmail Ads », *Bloomberg*, (23 June 2017), en ligne : <https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads>, (consulté le 28 avril 2019); Notons, que de nombreux articles sont disponibles sur ce sujet.
[240] 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,* p. 7; Raymond DORAY et François CHARRETTE, *Accès à l'information*, Cowansville, Éditions Yvon Blais, 2013 (mise à jour), p. III/ 70.1-1.
[241] OQLF., préc., note 10, « intégrité ».
[242] LCCJTI, art. 6; Cette définition est pratiquement identique à celle inscrite 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 ».

Heureusement pour les services infonuagiques, le protocole Internet par lequel transigent les données repose sur des technologies de correction d'erreur de paquets fournis par le Protocol TCP/IP[243]. Il s'avère donc presque impossible que l'intégrité des données en soit affectée d'autant qu'en droit, il existe la présomption prévue à l'article 30 de la LCCJTI prévoyant 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. »[244].

L'ensemble des fournisseurs infonuagique forceront également l'utilisation de connexions sécurisées à l'aide du protocole Transport Layer Security (TLS-SSL)[245] qui pourra être considérée comme un « moyen approprié » au sens de l'article 34[246] de la LCCJTI lorsque la classification des renseignements qu'il contient l'exige. Notons que, comme nous l'avons inscrit au risque R7, les grands fournisseurs d'infonuagique offrent maintenant des liens dédiés réseau permettant d'agrémenter leurs offres de service d'infrastructure sous forme de service. Cet atout, quoique lié principalement à la disponibilité, permettra notamment de borner les possibilités d'accès intrusifs pouvant affecter l'intégrité des données lors de leurs transits vers et depuis le nuage[247].

Dans le cas d'un dépôt de données infonuagique, il est sensiblement facile pour quiconque voulant vérifier que ses données n'ont pas été altérées, de valider avec une fonction

---

[243] Information Science Institute, University of Southern California, RFC : 793, « Transmission control protocol, protocol specification », en ligne <http://tools.ietf.org/html/rfc793>, (consulté le 28 avril 2019); Daniel POULIN, *L'autoroute de l'information et son potentiel pour le droit* dans Ghislain ROUSSEL (dir.), Autoroute de l'information en droit d'auteur : collision ou covoiturage, (Actes de la journée d'étude tenue à Montréal, le 18 novembre 1994), Montréal, ALAI-Canada, 1995, 6, 16.

[244] LCCJTI, art. 30.

[245] OQLF., préc., note 10, « Transport Layer Security » : « Protocole permettant d'assurer la protection du caractère confidentiel des données échangées entre un navigateur et un serveur Web. ».

[246] LCCJTI, art. 34. : « **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. ».

[247] Microsoft Corporation annonce sur leur site depuis juillet 2016 que « Les clients canadiens ont désormais la possibilité de créer des connexions privées au nuage. Les connexions Expressroute ne passent pas par l'Internet public, procurent une plus grande fiabilité, des débits plus rapides et des latences moindres par rapport aux connexions classiques sur Internet. » en ligne : <https://www.newswire.ca/fr/news-releases/microsoft-ouvre-le-nuage-canadien-pour-les-entreprises-578849601.html>, (consulté le 28 avril 2019).

de hachage[248] d'un fichier ou encore en inspectant ses métadonnées[249]. Par contre, cette vérification est plus complexe dans le cas d'une infrastructure complète puisqu'elle englobera des milliers de fichiers et d'informations qui transiteront constamment entre les clients et les services infonuagiques[250]. Certes, s'il n'y a pas d'usurpateur entre les points de connexion réseau, l'élément de cette triade n'en sera pas outre mesure affecté. Par usurpateur, nous entendons dire que la transmission des clés prévue pour sécuriser la communication doit se faire de manière confidentielle afin d'assurer que l'intégrité soit préservée[251].

Afin de pallier cette ambiguïté, les complices de l'intégrité sont sans aucun doute les journaux[252]. Ils contiennent tous les faits significatifs qui permettront de valider qu'aucun évènement[253] perturbateur n'ait altéré le contenu des infrastructures infonuagiques. Toutefois, nous l'avons soulevé au risque R.20, ces journaux doivent, bien entendu, être eux aussi intègrement conservés existants et accessibles par les administrateurs des infrastructures.

Dans l'intention d'accompagner les utilisateurs du nuage dans cette lourde tâche qu'est la journalisation des événements systèmes, le NIST a rédigé un guide de la gestion des journaux de sécurité informatique[254]. Bien que ce document n'ait pas été spécifiquement ciblé pour les services infonuagiques, il identifie les problèmes tels que la nécessité à assurer l'intégrité des

---

[248] Dans le *Règlement sur les signatures électroniques sécurisées DORS/ 2005-30*, la fonction de hachage est définie comme une « Opération mathématique unidirectionnelle électronique qui convertit des données contenues dans un document électronique en un condensé propre à ces données de sorte que, advenant toute modification de celles-ci, un condensé différent en résulterait. (*hash function*) ».

[249] OQLF., préc., note 10, « métadonnées » : « Donnée qui renseigne sur la nature de certaines autres données et qui permet ainsi leur utilisation pertinente. ». Voir notamment : Manuel MUNIER et Vincent LALANNE et Pierre-Yves ARDOY et Magali RICARDE, « Métadonnées & Aspects juridiques Vie Privée vs Sécurité de l'Information », 9ème Conférence sur la Sécurité des Architectures Réseaux et des Systémes d'Information (SARSSI'2014), May 2014, Saint-Germain-Au-Mont-d'Or, France. p. 69.

[250] Nous pourrions vérifier la valeur du hash ou les métadonnées d'un serveur virtuel, mais puisque ceux-ci sont en opération lors de leur entreposage sur les IaaS, leur valeur changera constamment ce qui empêche la vérification de l'intégrité même du fichier contenu sur serveur hôte.

[251] Dans le jugement *White* v *Graham*, 2017 ONSC 1268 la partie demanderesse ne pouvait plus, en raison de ce type d'attaque « *trust content via electronics* ».

[252] OQLF., préc., note 10, « journal » : « Relevé chronologique des opérations informatiques, constituant un historique de l'utilisation des programmes et des systèmes sur une période donnée. ».

[253] *Id*., « évènement » : « Signal qui permet, par ses différents états, d'indiquer la situation ou l'évolution d'une partie d'un système. ».

[254] Karen KENT, Murugiah SOUPPAYA, NIST, *Guide to Computer Security Log Management,* SP 800-92, Special Publication, Septembre 2016.

données, mais aussi des journaux eux-mêmes[255]. Les résultats des audits effectués par le fournisseur infonuagique ou des tierces parties ne seront pas d'emblée accessibles par les universités clientes du service[256].

L'un des principaux atouts de l'infonuagique, conséquemment de l'IaaS, est sans aucun doute la dématérialisation et par conséquent la résilience des infrastructures. Toutefois, ce principe s'accompagne d'un éparpillement des données qui ne vient pas sans conséquence. Il pourrait se rendre jusqu'à mettre en péril l'intégrité des infrastructures du nuage. Heureusement, comme nous le verrons, plusieurs articles de la LCCJTI font mention d'intégrité. C'est notamment le cas de l'article 4 qui prévoit que :

> « Un document technologique, dont l'information est fragmentée et répartie sur un ou plusieurs supports situés en un ou plusieurs emplacements, doit être considéré comme formant un tout, lorsque des éléments logiques structurants permettent d'en relier les fragments, directement ou par référence, et que ces éléments assurent à la fois l'intégrité de chacun des fragments d'information et l'intégrité de la reconstitution du document antérieur à la fragmentation et à la répartition.
>
> Inversement, plusieurs documents technologiques, même réunis en un seul à des fins de transmission ou de conservation, ne perdent pas leur caractère distinct, lorsque des éléments logiques structurants permettent d'assurer à la fois l'intégrité du document qui les réunit et celle de la reconstitution de chacun des documents qui ont été ainsi réunis. »[257].

Le traitement de l'information suggère également un degré d'immixtion important à la notion d'intégrité. De la même manière que pour la transmission, la notion de « traitement » est explicitement inscrite dans la définition de l'Office québécois de la Langue française[258]. Hélas, l'article 6 de la LCCJTI précitée ne contient pas de mention explicite quant au « traitement de l'information ». Néanmoins, nous admettrons que le traitement peut être implicite à la notion de « cycle de vie ». En comparaison aux simples dépôts de données infonuagiques, les IaaS seront non seulement appelées à entreposer ces données dans les nuages, mais elles devront aussi permettre le traitement de celles-ci.

---

[255] *Id.*, préc., note 254, p. 3-10.
[256] Claude BAUDOIN *et al*., préc., note 224, p. 12.
[257] LCCJTI, art. 4.
[258] OQLF., préc., note 10, « intégrité des données ».

Assurer l'intégrité lors du traitement de l'information n'est pas une mince affaire. Le chiffrement des données est une approche commune pour protéger la confidentialité des données inertes[259]. Toutefois, lorsqu'un travail est effectué sur des données, elles doivent être déchiffrées avant de permettre leur traitement[260]. Cette action pourra avoir de lourdes conséquences sur l'intégrité ou la confidentialité des données puisque, pour être possible, le serveur doit connaître cette clé. Il existera alors une possibilité de fuite de données déchiffrées, mais également la divulgation de la clé de chiffrement elle-même dans l'éventualité où le serveur serait compromis[261]. Afin de pallier cette vulnérabilité, deux possibilités s'offrent aux usagers de l'infonuagique. La première implique des utilitaires employant une technologie permettant le déchiffrement et le chiffrement des données du côté clients. De cette façon, les données resteront constamment inopérantes du côté de l'IaaS. Cependant, cette avenue bloque l'avantage de recourir à la puissance de l'infonuagique pour le traitement des données. L'autre possibilité plus intéressante permet le traitement de données chiffrées, mais les fonctions possibles seront restreintes à des recherches de base ou des requêtes limitées.[262] Ce procédé qui se limite souvent à effectuer des opérations algébriques sur des données chiffrées se nomme chiffrement homomorphe[263]. Les résultats de ces calculs restent chiffrés et ne peuvent être lus puis interprétés que par une personne ayant accès à la clé de déchiffrement.[264]

La notion d'intégrité traite également de la question de pérennité des données, d'ailleurs l'article 26 de la LCCJTI dit :

> « […] Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès […]. Il doit de même assurer le

---

[259] David P. WHELAN, *Practice Law in the Cloud,* Aurora*,* Canada Law book, 2013, p. 83.
[260] Eyad SALEH, Ahmad ALSA'DEH, Ahmad KAYED et Christoph MEINEL « Processing over encrypted Data : Between Theory and Practice » SIGMOD Record, September 2016 (Vol. 45, No. 3), p. 5.
[261] *Id*., p. 11.; Voir Annexe 1 : Analyse de Risque, R.15.
[262] *Id*., p. 12.
[263] Sashank DARA, « Cryptography Challenges for Computational Privacy in Public Clouds », International Institute of Information Technology, 2013, en ligne : <https://eprint.iacr.org/2013/272.pdf>.
[264] Pour plus d'information sur le chiffrement homomorphe : en ligne : <https://www.microsoft.com/en-us/research/project/homomorphic-encryption/#>.

respect de toute autre obligation prévue par la loi relativement à la conservation du document. »[265](nos soulignements).

La « période » et la « conservation » dont il est question dans cet article se voient bafouées par la permanence des données, telle que soulevée par le risque R.19. L'état de l'infonuagique actuel suggère que toute forme d'infrastructure aura une durée de vie dissimilaire. La raison est toute simple : aucun prestataire de service n'utilisera la même technologie pour l'écriture des données issues des infrastructures infonuagiques des universités[266] (ou de toute autre institution). Nous devons tout de même prendre en considération les systèmes existants et les nouveaux systèmes d'information.

Comme nous l'avons soulevé lors du premier chapitre, l'infrastructure sous forme de service réside habituellement sur un ensemble de machines virtuelles[267], communément appelées « VM » sur laquelle un administrateur peut installer une instance d'un système d'exploitation[268] de son choix et lui attribuer des rôles ou des services. Prenons par exemple le cas de Microsoft Azure[269]. Cet exploitant est l'un des rares à indiquer dans sa documentation publique les effets et le fonctionnement des écritures effectués sur ses services infonuagiques. Il y est écrit que :

> « […] *Virtual machines are stored in Storage as blobs[270] […]. When a VM is deleted, the space on disk that held the contents of its local virtual disk is marked as free, but is not zeroed. The space will eventually be used to hold data for some other object, but there is no upper bound on the amount of time the obsolete contents may stay there. The virtualization mechanism, however, is designed to ensure that those spots on the disk cannot be read by another customer (or even*

[265] LCCJTI, art. 26.
[266] Voir notamment : Motasem ALDIAB, Cloud Academy, « Public Cloud War: AWS vs Azure vs Google », en ligne <https://cloudacademy.com/blog/public-cloud-war-aws-vs-azure-vs-google/>, Dans cette publication Microsoft Azure enregistre les « machine virtuelle » dans un mode Blobs (Microsoft's Block Storage option), GCP utilise du « persistent disks » et AWS utilise le mode EBS(Amazon Elastic Block Store).
[267] OQLF., préc., note 10, « machine virtuelle » : « Environnement informatique séparé, autonome et complet, qui est virtuellement créé à partir d'une allocation dynamique de ressources logicielles ou matérielles disponibles sur un ou plusieurs serveurs. ».
[268] *Id*., « System d'exploitation ».
[269] Microsoft Azure : est la plateforme sur laquelle réside les infrastructures sous forme de service chez Microsoft.
[270] Binary Large OBject (BLOB) Nous pouvons le définir comme un type de donnée permettant le stockage de données binaires dans le champ d'une table d'une base de données.

*the same customer) until data is written again, thus ensuring there is no threat of data leakage.* »[271] (nos soulignements).

Bref, les données resteront sur le stockage lié à l'IaaS pour une durée indéterminée. Même si Microsoft mentionne l'obstruction d'accès du mécanisme de virtualisation, comme nous l'avons soulevée préliminairement, plusieurs risques (R10, R13, R16) pourraient compromettre les infrastructures infonuagiques et par conséquent les possibles renseignements personnels qu'elles renferment pour ainsi contrevenir à l'article 63.1 de la *Loi sur l'accès* préalablement cité.

Pour conclure cette sous-section, des mécanismes de même que des bonnes pratiques existent pour remédier à la problématique de l'intégrité des documents entreposés et transmis sur une infrastructure sous forme de service. La vérification des sommes de contrôle[272] ou le fait de scruter au crible les évènements système permettront de démontrer que toutes les précautions ont été prises afin de répondre à l'obligation d'intégrité recherchée. Ainsi, il sera au moins possible d'éviter le traitement ultérieur des données ou encore l'utilisation d'une infrastructure sachant qu'elle a été compromise[273]. Évidemment, cette obligation reviendra tant à l'université, qu'au prestataire de l'infrastructure sous forme de service.

### 2.3.2 La disponibilité

Finalement, complétons ce chapitre avec le troisième élément de la triade, soit la disponibilité. Ne s'agit-il pas de la prémisse de l'infonuagique ? L'ubiquité des données : elles sont disponibles partout, tout le temps[274]. Il en va de même pour le modèle de prestation de service qui nous intéresse. Effectivement, l'infrastructure en tant que service offre la possibilité, comme nous l'avons vu au préalable, de prendre en charge une partie ou l'entièreté des infrastructures liées à l'informatique des universités. Par exemple, dans le cadre des connexions

---

[271] Walter MYERS III, « Microsoft Azure Data Security (Data Cleansing and Leakage », Microsoft Developer, Septembre 2014, en ligne : <https://blogs.msdn.microsoft.com/walterm/2014/09/04/microsoft-azure-data-security-data-cleansing-and-leakage/>, (consulté le 28 avril 2019).
[272] OQLF., préc., note 10, « checksum » : « Somme calculée non pour sa valeur numérique intrinsèque, mais afin de vérifier l'intégrité des données de contrôle qui ont servi à l'établir. ».
[273] Tobias ACKERMANN, *IT Security Risk Management*, Springer Gable, 2013, p. 45.
[274] R. SAMANI, J. REAVIS et B. HONAN, préc., note 37, p. 2; Pierre TRUDEL *et al*., préc., note 1, p. 1-17.

vers les services, les administrateurs responsables d'un réseau pourraient répliquer leur service LDAP[275]. Ce qui aurait pour effet, lors d'une panne locale des infrastructures régissant l'accès aux ressources, de préserver l'accès à celles-ci puisque le lien authentifiant serait intégralement basculé[276] vers la partie du service disponible depuis Internet. En prévision de pallier un besoin épisodique de grande demande de performance dans le cas de calcul scientifique, une université pourrait également utiliser les services d'infrastructures en tant que service de Calcul Canada[277] ou d'un service infonuagique public[278]. Comme nous l'avons déjà soulevé, tous les services infonuagiques offrant la possibilité d'héberger des infrastructures traiteront de ce que nous appelons des « données », que ce soit un système d'exploitation ou des informations confidentielles, elles seront toutes conservées et transiteront vers les nuages sous la forme de données[279].

La disponibilité des données, ou l'accès à l'information, est la « Propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite. »[280]. Cette propriété essentielle pour le monde universitaire est imposée par la loi. En effet, l'article 19 de la LCCJTI dispose 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 »[281]. Cette conformité concernant la conservation des documents aura bien entendu un lien causal avec les propriétés de consultation définies à l'article 23 de la même loi qui précise

---

[275] OQLF., préc., note 10, « LDAP » : « Protocole de gestion d'annuaires, permettant à des clients Internet d'accéder automatiquement à des services d'annuaires en ligne sur TCP. ».
[276] *Id*., préc., note 35.
[277] Voir Calcul Canada, en ligne : <https://www.computecanada.ca/page-daccueil-du-portail-de-recherche/acces-aux-ressources/?lang=fr>, « Calcul Canada s'applique à fournir une plateforme de calcul informatique de pointe (CIP) qui répond aux besoins de sa communauté d'utilisateurs aux profils très divers. En plus du soutien existant pour les projets de recherche d'envergure, la plateforme nationale de CIP du Canada est capable d'appuyer des activités de recherches exigeantes pour des projets de petite ou moyenne taille à grand volume de données, quelle que soit la discipline. ».
[278] *Id*., préc. Note 117.
[279] OQLF., préc., note 10, « donnée » : « Représentation d'une information, codée dans un format permettant son traitement par ordinateur. ».
[280] *Id*., « Disponibilité ».
[281] LCCJTI, art. 19.

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 »[282].

Afin de permettre d'effectuer ses fonctions sans interruption, les infrastructures sous forme de service utiliseront des technologies permettant entre autres la haute disponibilité[283]. Cette caractéristique permet aux infrastructures de rester disponibles en tout temps, empêchant les interruptions de service dû aux nombreux risques énumérés précédemment.

Dans d'autres cas, certains risques peuvent tout de même avoir des effets sur l'obligation de disponibilité. Le problème le plus important reste néanmoins que le client n'exerce que très peu de contrôle sur la disponibilité des données. Il pourra cependant pallier ce désagrément par la conservation d'infrastructures locales ou par une « Entente écrite entre un fournisseur de service et un client où sont consignés les niveaux de service pour un service donné. »[284], communément appelé un accord sur les niveaux de service ou « *SLA* ». Heureusement, les grands exploitants de centres de données offrent maintenant des garanties impressionnantes en ce qui a trait aux opérations et à l'accessibilité de leurs services dans ces ententes de bases. Ces ententes « *SLA* » ont d'ailleurs été normalisées récemment par l'ISO[285] afin de définir des objectifs de niveau de service relatifs à : la performance, la sécurité, la gestion des données ainsi que les données à caractères personnelles[286].

Pour exemple Microsoft avec sa plateforme Azure garantie que lorsque deux instances de rôle[287] ou plus sont déployées dans différentes occurrences de machine virtuelle, si les mises à jour de plateforme sont appliquées simultanément par le prestataire de service, au moins une des instances de rôle aura une connectivité garantie 99,95% du temps. Dans la négative, des

---

[282] *Id*., art. 23.
[283] OQLF., préc., note 10, « Hautes disponibilité » : « Qualité d'un système, ou d'une partie d'un système (ex. : un périphérique), dont le pourcentage de temps durant lequel on peut l'utiliser est très élevé par rapport au temps global où il est en demande. ».
[284] *Id*., « Service Level Agreement ».
[285] Norme ISO/IEC 19086-2016, « Cloud Service Level Agreement standardisation guidelines», Organisation Internationale de Normalisation (ISO), Genève.
[286] *Id*.
[287] Par rôle ou service de serveur, nous signifions par exemple différent service informatique : LDAP, DNS, DHCP, ou autres.

crédits seront appliqués au compte de l'entreprise[288]. Une indisponibilité des services est une chose alors que l'indisponibilité des données entreposées sur ces infrastructures en est une autre. Nulle mention à cet effet n'a été identifiée aux contrats de service que nous avons étudiés.

Toutefois, plus de disponibilité évoque essentiellement une structure complexe englobant des technologies de réplications des données sur différents sites[289].


Figure 9. Carte des "Régions Azure" de Microsoft en 2019

Par exemple, dans l'édition de l'entente « Google for Education ». Il est spécifié que :

> « […] Dans le cadre de la fourniture du Service, Google peut stocker et traiter des données de clients aux États-Unis (où dans n'importe quel autre pays où Google ou ses agents possèdent des installations. En utilisant les Services, le client consent à ce transfert, le traitement et le stockage des données clients. »[290] (notre traduction).

L'emplacement des données, virtuellement impossible à définir, pose un problème sérieux lorsque vient le temps de traiter des litiges. Il est difficile d'identifier à quelle juridiction

---

[288] Voir notamment le « Service Level Agreement Microsoft Azure » en ligne : <https://azure.microsoft.com/en-us/support/legal/sla/summary/> ; Le « Google Compute Engine Service Level Agreement », en ligne : < https://cloud.google.com/compute/sla>; ainsi que le « Amazon Compute Service Level Agreement », en ligne : < https://aws.amazon.com/compute/sla/>, (consulté le 28 avril 2019); Dans lesquels il est stipulé exactement le même niveau de disponibilité mensuelle aux clients.

[289] Microsoft 2019, en ligne : <https://azure.microsoft.com/en-ca/regions/ >, (consulté le 28 avril 2019).

[290] Entente de service intervenue entre Google Inc. et The Chancellor, Masters, and Scholars of the University of Cambridge. 2010.

l'on doit associer les données lorsqu'une panne survient. Google, par exemple, possède des Centres de données dans des pays n'offrant pas d'équivalence dans la protection requise par la *Loi sur l'accès.* À l'heure actuelle, il n'y a pas de jurisprudence en quantité suffisante sur la question de l'infonuagique pour établir une responsabilité aux manquements pouvant survenir au requis de nos lois. D'autant plus que, lorsqu'une brèche de sécurité ou une coupure survient, ce sont des accords généraux concernant le service (SLA) qui s'appliquent. Il n'y a, à l'ordinaire, aucun accord individuel ou de conditions additionnelles possibles avec les universités telles qu'il en est possible avec d'autres grandes institutions comme les banques[291].

D'autre part, en ce qui a trait à la disponibilité des données, les universités ont habituellement deux niveaux d'accès Internet. Tous deux offerts par le RISQ (Réseau d'information Scientifiques du Québec[292]), ils permettent un accès intranet interuniversités ainsi qu'un accès vers l'Internet commercial. Dans certains cas, une réplication des serveurs sur l'intranet est effectuée dans le but de garantir une rapidité optimale aux requêtes les plus souvent opérées. Par contre, à moins de faire l'acquisition d'une connexion directe[293] avec le fournisseur, les liens vers les infrastructures infonuagiques seront desservis par les liens Internet commerciaux. Quoique très performants, ces liens Internet sont très onéreux pour les universités et surtout aucunement infaillibles. Par ailleurs, en déportant des infrastructures, l'université sera facturée pour l'utilisation de la bande passante supplémentaire. Cette action sera inévitable puisqu'elle sera requise au bon fonctionnement de ses services, contrairement à l'utilisation de la partie scientifique desservie par le fournisseur d'accès.

Au même titre qu'une infrastructure conventionnelle, la disponibilité des infrastructures sous forme de service peut être influencée, tel que nos risques le démontrent, par une série de facteurs liés à des vulnérabilités d'ordre logicielles. Malgré qu'aucune loi ne l'impose

---

[291] Les services infonuagique ont intérêt à répondre à tous les critères de protections requis par le PCI Security Standard council, par exemples. Voir notamment : Michel COCHRAN et Paul D. WITMAN, « Gouvernance and service level agreement issues in a cloud computing environment », Journal of Information Technology Management Volume XXII, Number 2, 2011 en ligne : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.6370&rep=rep1&type=pdf (consulté le 28 avril 2019).

[292] Le RISQ « est un organisme à but non lucratif qui gère le réseau privé de l'éducation et de la recherche au Québec », en ligne : <http://www.risq.qc.ca/>, (consulté le 28 avril 2019).

[293] *Id.*, préc., note 247.

explicitement[294], plusieurs politiques encadrent la sécurité des infrastructures des technologies de l'information en suggérant qu'elles doivent « […] être soutenue par des outils, des pratiques et des mesures de surveillance et de mise à jour continue des systèmes d'exploitation, des principaux logiciels et de l'équipement […] »[295].

> Ajoutons notamment : « […]
> - l'installation continue des mécanismes de correction mis sur le marché par les fournisseurs;
> - une analyse annuelle des risques liés aux technologies de l'information;
> - des tests de vulnérabilité récurrents et des tests d'intrusion annuels sur les réseaux interne et externe. »[296].

Par souci de remédier à cette problématique, les fournisseurs de service offrent, puis contraignent dans certain cas, la distribution et l'installation de mises à jour logicielles[297]. Or, cette pratique, quoique recommandée, peut occasionner des incompatibilités et des pertes de disponibilité des instances en place chez un fournisseur de service. Néanmoins, ces mises à jour orchestrées permettront de se soustraire à beaucoup de vulnérabilités issues du monde des TI. Notamment, certains rançongiciel[298] qui pourraient utiliser ces vulnérabilités pour affecter un service. Ces rustines[299] ne serviront malheureusement à rien dans les cas d'arnaques utilisant l'ingénierie sociale. De plus, il n'est pas certain que l'entreprise utilisant le service d'IaaS pourra effectuer les tests d'intrusion qu'elle devrait pourtant pouvoir faire[300].

---

[294] En effet certaines lectures des disposition de la LCCJTI l'impose, mais cette lectures n'a pas été soumise devant les tribunaux.

[295] Cet extrait est issu de la politique du GUVERNEMENT DU QUÉBEC, MERN - Ministère de l'Énergie et des Ressources naturelles du Québec, (mai 2015), en ligne : <https://www.mern.gouv.qc.ca/publications/ministere/politique/securite-information.pdf>, mais elle résume essentiellement en une phrase les propos du *GOUVERNEMENT DU QUÉBEC, Conseil du Trésor, « Cadre gouvernemental de gestion – Sécurité de l'information », (Juin 2014), en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_securite_information.pdf>, (consulté le 28 avril 2019).*

[296] *Id*.

[297] Shantanu SRIVASTAVA, « Maintenance for virtual machines in Azure », Microsoft Azure, Décembre 2018, en ligne : <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/planned-maintenance>, (consulté le 28 avril 2019).

[298] OQLF., préc., note 10, « rançongiciel » : « Logiciel malveillant qui permet de verrouiller un ordinateur ou de chiffrer ses données dans le but d'extorquer de l'argent à son utilisateur avant de lui en rendre l'accès. ».

[299] *Id*., « rustine » : « 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. ».

[300] Microsoft Azure offre la possibilité (après avoir avertis Microsoft) de permettre des tests d'intrusion vers nos infrastructures soutenues par leur réseau.

Il importe de souligner que plusieurs risques énumérés à la section précédente[301] sont propres ou accentués par l'utilisation des infrastructures sous forme de service. Qui plus est, malgré la haute disponibilité annoncée par les prestataires de service infonuagique[302] nous devons mettre en évidence que :

> « […] l'accès [aux infrastructures sous forme de service] est contrôlé par un tiers qui pourrait – volontairement ou par erreur – retirer des permissions ou des droits d'accès, voir même retenir des données pour faute de paiement ou toute autre raison qu'il considère légitime. »[303].

Il est essentiel que les clients des services d'IaaS emploient des politiques de même que des pratiques pour effectuer des sauvegardes de qualités et mettent en place un plan de relève efficace qui pourra être utilisé advenant que les instances de ces services soient supprimées, perdues, corrompues, détruites ou tout simplement non accessible[304].

Qu'adviendra-t-il des données ou des instances de serveurs virtuels si le contrat avec le prestataire de service est rompu ? Ces éléments doivent être pris en considération autant que possible dans le choix du prestataire de service en plus d'être spécifiés dans un contrat d'accord sur les niveaux de service (SLA).

La disponibilité évoque d'assurer un accès opportun et fiable à l'information, ainsi que dans notre cas précis, à l'IaaS. Par contre, pour permettre à l'infonuagique d'atteindre leurs objectifs de protéger et d'exploiter les ressources informationnelles des organisations[305] tout en respectant les prérequis en matière de disponibilité ou les risques inhérents associés, les universités auraient avantage à recourir à un modèle communautaire ou un modèle hybride d'infrastructure sous forme de service. De cette manière, ils pourraient désigner des responsables de la gestion des différentes composantes de l'infrastructure critique sans omettre d'accorder des rôles et des responsabilités conformément à leurs obligations légales et réglementaires.

---

[301] Voir Annexe 1 : Analyse de Risque; Nous référons notamment aux risques suivants: R.1, R.2, R.3, R.4, R.5, R.6, R.8, R.9, R.10, R.20.
[302] *Id.*, préc., note 283.
[303] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 85.
[304] R. SAMANI, J. REAVIS et B. HONAN, préc., note 30, chap 5, p. 109.
[305] Jerry ARCHER *et al*., « Security Guidance for critical areas of focus in cloud computing v.3.0», CSA, 2011, en ligne : <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>, (consulté le 28 avril 2019).

À la lumière de tout ce qui précède, nous croyons qu'il serait, préférable pour veiller au respect des obligations de sécurité des données, de préconiser un fournisseur canadien d'infonuagique ou encore d'opter pour une option permettant de recourir à une portion canadienne d'un nuage chez un des grands fournisseurs de service en nuage.

> « *With Microsoft Azure you have the ability to select the Canadian region where your data is stored, so your assets stay right where you need them.* »[306].

Néanmoins, une étude approfondie des conditions d'utilisation nous permettra de rapidement constater que la souveraineté numérique des données en sera tout de même entachée. En effet, l'emprise que gardera le géant informatique américain sur les infrastructures ainsi maintenues leur permettra de mener une surveillance et d'accéder aux données pour détecter et prévenir de possibles actes de terrorisme.

> « *This creates a situation in which a Canadian company, which has data in Canada and is doing business only in Canada, might be subject to the legal jurisdiction of another country.* »[307].

Nous l'avons vu, l'obligation de sécurité comporte des conditions particulières parfois critiques et laborieuses à respecter. Les normes et certaines lois en sont pour beaucoup. La question demeure : dans quelle condition juridique une université peut-elle adopter une infrastructure sous forme de service? C'est ce que nous aborderons en seconde partie de ce mémoire.

---

[306] Microsoft permet effectivement de limiter l'utilisation d'infrastructure situé uniquement au Canada. en ligne : <https://www.microsoft.com/en-ca/sites/datacentre/enterprise.aspx>, (consulté le 28 avril 2019).
[307] Sherweb | Blog, « Microsoft Azure's Canadian Cloud Servers : A True Canadian Cloud? », 10 juin 2016, en ligne : <http://www.sherweb.com/blog/azure-canadian-cloud/>, (consulté le 28 avril 2019).

# SECONDE PARTIE : Le cadre juridique applicable à l'utilisation de l'infrastructure sous forme de service

Comme nous l'avons soulevé dans la première partie de ce mémoire, l'obligation de sécurité liée à l'utilisation de l'infonuagique est bien entendu encadrée par des normes techniques et des politiques, mais elle découle également de plusieurs dispositions issues de la loi. Nous verrons aussi que le domaine universitaire auquel se greffe graduellement l'utilisation de l'IaaS est un environnement hybride. Son édification partage des notions provenant des dispositions applicables aux institutions publiques ainsi que de celles qui visent aux entreprises privées. C'est dans cette seconde partie que nous évoquerons l'orientation que prennent les lois de ces deux secteurs à l'endroit de l'obligation de sécurité liée à l'utilisation d'infrastructures sous forme de service par le milieu universitaire. Dans cette section, nous décrirons d'abord les règles obligataires spécifiques à son utilisation relativement au droit public (Chapitre I) puis nous aborderons le pendant privé des contraintes législatives encadrant l'exploitation de l'IaaS (Chapitre II).

## Chapitre I. Les obligations découlant des lois applicables aux organismes publics

L'université est une institution publique, elle est bien entendu assujettie prioritairement aux lois de ce secteur. Dans ce chapitre, nous analyserons l'incidence du droit public en ce qui a trait aux éléments issus du précédent chapitre, à savoir : les types de données, leurs classifications, ainsi que leurs effets sur la triade qui suscite notre intérêt depuis le commencement de ce mémoire, c'est-à-dire la confidentialité, l'intégrité, et la disponibilité. En outre, nous sillonnerons les cas d'application du cadre législatif public en vigueur. Tel que soulevé précédemment, nous ferons souvent référence à des données informatiques, mais réitérons sur le fait que l'IaaS s'avère bien plus importante que de simples espaces de dépôt de données. N'eût été le développement de ces derniers, l'engouement de l'infonuagique dans les universités ne serait certainement pas tel.

## 1.1 Les types de données visées par les lois applicables aux organismes publics

C'est principalement la *Loi sur l'accès* qui a su pérenniser l'importance des données des organismes publics au sens de la loi. Ironiquement, cette loi n'est pas rattachée directement aux technologies de l'information, mais sa préoccupation concernant les documents des organismes publics[308], communément sous forme de données informatiques, tisse les liens vers des lois plus spécifiques se rattachant aux éléments de la triade CID. Nous y reviendrons. D'emblée, la *Loi sur l'accès* énonce à son article 9 que « Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public. »[309]. Donc, à première vue, nous pourrions croire que l'utilisation d'infrastructure sous forme de service, malgré qu'elle pourrait mettre en lumière les documents universitaires, ne cause pas de grands soucis puisque ces documents peuvent de toute évidence être accessibles à quiconque fait la demande. Il est tout de même important de rappeler que tous les types de données présentes dans les universités ne seront pas assujettis à un tel droit d'accès.

Tel que vu précédemment, dans nos institutions d'enseignements, cinq grands types de données sont présentes : celles issues de la recherche[310], de l'enseignement[311], de la gestion de l'établissement[312], les données concernant les étudiants[313] ainsi que les données touchant les membres du personnel[314]. C'est dans cette section que nous procéderons à l'analyse de ces types de données et que nous verrons quelles règles juridiques dictent leurs fondements afin de permettre ou pas leurs traitements dans des IaaS.

---

[308] *Loi sur l'accès*, art. 67.2 al. 2.
[309] *Id*., art. 9.
[310] Voir PREMIÈRE PARTIE, chapitre 2, section 2.1.1.
[311] *Id*., section 2.1.2.
[312] *Id*., section 2.1.3.
[313] *Id*., section 2.1.4.
[314] *Id*., section 2.1.5.

### 1.1.1 Le traitement des données de recherche en vertu des lois applicables aux organismes publics

En premier lieu, observons les données de recherche « issues de l'observation, de l'expérimentation ou dérivées de sources existantes qui sont analysées en vue de produire ou de valider des résultats de recherche originaux. »[315]. Est-il juridiquement raisonnable de traiter ces données à même une IaaS? En grande partie[316], les investissements majeurs permettant de financer ces données proviennent d'organismes subventionnaires fédéral ou provinciaux[317]. Bien entendu, étant financées avec des deniers publics, elles se doivent d'être traitées en conformité avec les politiques, les normes ainsi que les obligations éthiques, commerciales et juridiques. Par conséquent, elles devront se soumettre aux lois applicables aux organismes publics.

À cet égard, la déclaration de principes des trois organismes fédéraux[318] sur la gestion des données numériques[319] prévoit que :

> « Les données doivent être gérées conformément aux normes et aux pratiques exemplaires les plus appropriées et pertinentes, lesquelles évoluent rapidement.[…] Il faut normalement préserver les données résultant du financement d'un organisme sur une plateforme ou dans un dépôt publiquement accessible, sécurisé et structuré, afin que d'autres chercheurs puissent les trouver et s'en servir. » [320] (nos soulignements).

Comme nous le constatons dans cet énoncé, l'institut de recherche en santé du Canada (IRSC), le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines (CRSH) sont des organismes conscients de

---

[315] *Id*., note préc. 129.
[316] Fédération Québécoise des professeures et professeurs d'université, « The funding of University Research in Quebec : Evolution and Challenge », Abstract, Février 2016. En ligne : <http://fqppu.org/le-financement-de-la-recherche-universitaire-au-quebec-evolution-et-enjeux/>, (consulté le 28 avril 2019).
[317] Les principaux organismes provinciaux sont le FRQ-NT, le FRQ-SC, le FRQ-S, le IRSST, le MDEIE. Leurs homologues fédéraux subventionnaires sont le CRSNG, le CRSH, l'IRSC, le CRC, la FCI ainsi que Le CRDI.
[318] L'instituts de recherche en santé du Canada (IRSC), le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines (CRSH).
[319] Gouvernement du Canada, « Déclaration de principes des trois organismes sur la gestion des données numériques », en ligne <http://www.science.gc.ca/eic/site/063.nsf/fra/h_83F7624E.html?OpenDocument>, (consulté le 28 avril 2019).
[320] *Id*.

l'évolution des technologies de l'information, du moins, ils en font mention dans leurs principes. Ils nomment d'ailleurs les caractéristiques « Accessible, sécurisé et structuré » pour qualifier l'ensemble des prescriptions techniques normalement imposées lorsque le financement provient d'un des trois organismes[321]. Ces éléments rappellent bien évidemment certains des objectifs de la triade CID et comme dans cette déclaration, plusieurs textes de loi viendront leur faire référence. À première vue, les adjectifs employés sont tout compte fait harmonisés avec les caractéristiques de l'infonuagique énoncée en début de travail[322]. Cependant, les données de recherches sont susceptibles de contenir des informations provenant de pratiquement tous les types de classification des données présentes dans les universités[323], à savoir : les données publiques, les données internes/privées, les données confidentielles, les données à accès restreint. Nous éluciderons dans la prochaine section l'incidence des infrastructures sous forme de service sur chacune de ces classifications des données.

En outre, puisque certaines activités de recherche sont financées par des fonds des trois organismes fédéraux de recherche, ils n'ont d'autres choix que de se soumettre à ce que la déclaration de principe dicte, et cette déclaration est sans équivoque, elle rappelle l'importance du regroupement des ressources informationnelles. Cette composante est issue notamment de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*[324]. Cette loi est l'une de celle régissant les directives de l'utilisation des technologies de l'information dans les universités recevant des fonds fédéraux. Cette loi a pour but entre autres « 2° d'optimiser les façons de faire en privilégiant le partage et la mise en commun du savoir-faire, de l'information, des infrastructures et des ressources; »[325] (nos soulignements). Ces principes de partage et de mise en commun sont des caractéristiques déterminantes de l'infonuagique[326] et bien évidemment de l'infrastructure sous forme de service. Cependant, il faut noter que les projets en ressources informationnelles de recherche et

[321] *Id*.
[322] Voir PREMIÈRE PARTIE, chap. 1, section 1.1 « La définition et les caractéristiques des services infonuagiques », p. 8.
[323] Voir PREMIÈRE PARTIE, chap. 2, section 2.2 « La classification des données présentes dans les universités».
[324] *Id*., préc., note 3.
[325] *Id*., préc., note 3.
[326] Voir section 1.2 « Caractéristiques distinctives de l'infonuagique », p. 9.

d'enseignement ne sont pas soumis à cette loi[327]. Il en est autrement des infrastructures ayant comme fonction la gestion de l'établissement[328], les données concernant les étudiants[329] ainsi que les données touchant les membres du personnel[330] lesquels pourront être influencés par ces lois spécifiant les règles de gouvernance et de gestion des ressources informationnelles.

Dans d'autres sphères de la recherche universitaire, certaines données de recherches sont financées par des partenariats industriels ou par le biais de financements mixes. Les obligations assujetties à ces données seront alors traitées différemment. Ils feront parfois appel à des règles de droit provenant du privé. Cette question sera précisée dans le prochain chapitre. Autrement, la règle la plus rigoureuse devra être mise en application. De plus, les obligations liées aux partenariats industriels ou commerciaux seront souvent encadrées par des obligations contractuelles et par des ententes de confidentialités (NDA). À cet effet, il importe de faire mention que l'article 23 de la *Loi sur l'accès* dispose :

> « 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. »[331] (nos soulignements).

La jurisprudence mentionne les conditions suivantes pour satisfaire cet article :

« […]

- Les renseignements ont été fournis par le tiers;
- Il s'agit de renseignements industriels, financiers, commerciaux, scientifiques, techniques ou syndicaux;
- La nature confidentielle de ces renseignements est démontrée objectivement;
- Ces renseignements sont habituellement traités de manière confidentielle par le tiers (critère subjectif). »[332] (nos soulignements).

---

[327] *Id*., préc., note 3. Art. 16.3 al. 2. « … Ne constitue toutefois pas un projet en ressources informationnelles un projet de recherche et de développement technologique réalisé dans le cadre de travaux d'enseignement ou de recherche menés sous l'égide d'un professeur, d'un chercheur, d'un chargé d'enseignement, d'un étudiant, d'un stagiaire, d'un technicien ou d'un professionnel de recherche au sein d'un établissement universitaire visé au paragraphe 4.1° du premier alinéa de l'article 2. ».

[328] Voir PREMIÈRE PARTIE, chap. 2, section 2.1.3 « Les données de gestion », p. 38.

[329] Voir PREMIÈRE PARTIE, chap. 2, section 2.1.4 « Les données concernant les étudiants », p. 39.

[330] Voir PREMIÈRE PARTIE, chap. 2, section 2.1.5 « Les données concernant les membres du personnel », p. 40.

[331] *Loi sur l'accès*, art. 23, aussi, les articles 22, 24 et 25 seront en lien avec bien des projets de recherches universitaires dans lequel des tiers (entreprises privées) externes à l'édification publique sont impliqués.

[332] *ATMS inc*. c. *Centre hospitalier de l'Université de Montréal*, 2018 QCCAI 80.

Puisque les projets de recherche comportant des renseignements liés à ces conditions sont souvent appuyés par des contrats engageant les parties, le caractère objectif de la confidentialité est clairement établi. C'est pour cette raison qu'il ne serait pas raisonnable de traiter ces données sur une infrastructure sous forme de service sans avoir avisé et avoir obtenu au préalable l'accord du tiers impliqué dans le projet de recherche.

Calcul Canada, un grand fournisseur de service de calcul scientifique dédié à la recherche universitaire, préconise la possession d'infrastructure et dévalorise l'utilisation des services commerciaux pour différente raison, notamment au point de vue des coûts[333]. De plus, il demeure quand même que Calcul Canada se dit interagir avec les services commerciaux ayant une approche hybride pour offrir « …les avantages possibles de variation dans l'équilibre des services. »[334]. Il va sans dire que le gouvernement fédéral a beau investir 572,5 millions pour les 5 prochaines années dans l'infrastructure de Calcul Canada[335], en comparaison, les analystes s'accordent pour estimer les dépenses sur les biens et l'équipement chez Microsoft à croître de 20% en 2019 à près de $14 milliards[336] pour l'infrastructure associée à l'infonuagique.

Depuis quelques années déjà, les gouvernements fédéral et provinciaux s'accordent pour que les institutions d'enseignement et les centres de recherches aient recours aux instances informatiques de Calcul Canada afin d'économiser des ressources et d'éviter de gaspiller les fonds publics en partageant les solutions TI. C'est d'ailleurs ce que spécifie l'article 4.6.4 du « guide des politiques et des programmes 2017 » :

> « La FCI s'attend à ce que l'infrastructure de calcul informatique de pointe soit hébergée, gérée et coordonnée par Calcul Canada. Ainsi, un établissement qui désire demander ce type d'infrastructure doit préparer sa proposition en

---

333 Calcul Canada, « L'infonuagique pour les chercheurs », (Décembre 2016), en ligne : <https://www.computecanada.ca/wp-content/uploads/2015/03/CloudStrategy2016-2019-forresearchersEXTERNALFrCa.docx.pdf>, (consulté le 28 avril 2019).

334 *Id*.

335 Par infrastructure, on entend ici l'ensemble des ressources qu'offre Calcul Canada à ses chercheurs universitaires, il ne s'agit pas d'investissement uniquement dans leurs projets d'infrastructure infonuagique. Voir à cet effet Calcul Canada, « compute canada applauds $572.5 million investment in digital research infrastructure », Février 2018, en ligne : <https://www.computecanada.ca/featured/compute-canadas-applauds-572-5-million-investment-in-digital-research-infrastructure/>; et William Francis MORNEAU, Ministre des Finance, « Égalité Croissance, une classe moyenne forte », Février 2018, en ligne : <https://www.budget.gc.ca/2018/docs/plan/budget-2018-fr.pdf>, (consulté le 28 avril 2019).

336 Eric JHONSA, «Amazon's Spending on the Cloud is Growing, but Not Nearly as Fast as Facebook's», *TheStreet, Août 2018, en ligne :* <https://www.thestreet.com/technology/amazons-cloud-capital-spending-is-growing-but-not-as-fast-as-facebooks-14678361>, (consulté le 28 avril 2019).

consultation avec Calcul Canada (veuillez visiter le site Web de Calcul Canada pour obtenir de l'information sur le processus en place pour faciliter la collaboration avec les établissements). L'infrastructure de calcul informatique de pointe comprend normalement des ressources ou des systèmes tels que :

- systèmes à forte capacité dédiés aux calculs séquentiels;
- systèmes dédiés aux applications parallèles requérant une communication à très haut débit;
- systèmes à mémoire partagée;
- systèmes dédiés aux applications requérant une grande quantité de mémoire;
- stockage à haute performance;
- archivage;
- informatique en nuage;
- systèmes comportant des cartes accélératrices, y compris des cartes graphiques;
- systèmes de visualisation de haute performance;
- systèmes dédiés au calcul orienté et interactif. »[337].

Comme nous pouvons le constater, « L'infrastructure de calcul informatique » comprend les systèmes associés à l'infonuagique, et ça va de soi, puisque Calcul Canada offre des services de calcul haute performance qui s'apparentant aux modèles de Logiciels sous forme de services (SaaS). De plus, ils offrent aussi aux chercheurs des systèmes d'infrastructure sous forme de service[338]. Ces systèmes issus d'investissements gouvernementaux seraient fortement à envisager dans le cas où les centres universitaires de recherche voudraient céder un segment de leur infrastructure à un tiers.

Finalement, les données de recherches sont également assujetties à la *Loi sur les archives*[339], cette loi provinciale ainsi que le chapitre 3 de l'énoncé de politique des trois Conseils, lorsque les investissements proviennent en partie du gouvernement fédéral, de même que certains règlements internes propres aux établissements viendront encadrer la conservation

---

[337] Fondation Canadienne pour l'Innovation, « Guide des politiques et des programmes, 2017 » en ligne : <https://www.innovation.ca/sites/default/files/essential_documents/guide_des_politiques_et_des_programmes_de_la_fci-sommaire_des_principales_modifications_2017.pdf>, (consulté le 28 avril 2019).
[338] Voir notamment Calcul Canada, Research Portal, en ligne : <https://www.computecanada.ca/page-daccueil-du-portail-de-recherche/acces-aux-ressources/glossaire-technique/?lang=fr>, (consulté le 28 avril 2019).
[339] *Loi sur les archives*, L.R.Q., chapitre A-21.1., art. 6.

de l'information liée à certains types de recherche universitaire, par exemple les données concernant certains renseignements personnels[340].

Il nous apparaît donc impensable que de telles données puissent être traitées à même une infrastructure sous forme de service du modèle public offert par une entreprise du secteur privé, puisque les données, les travaux, les calculs résultant de ces données de recherches pourront être interceptés par les tiers offrant les services d'infrastructure infonuagique.

### 1.1.2 Le traitement des données d'enseignements en vertu des lois applicables aux organismes publics

Lorsqu'on parle de données universitaires, ce sont souvent celles reliées à l'enseignement auquel nous pensons. Selon notre point de vue, il s'agit probablement des données les plus prédisposées à être utilisées sur des infrastructures sous forme de service. Tel que mentionné à même le second chapitre, ces données sont habituellement liées par une obligation à être conservé pour un temps donné[341] et sont souvent accessibles au grand public depuis les sites web des institutions ou du moins aux inscrits ainsi qu'aux employés via des plateformes d'apprentissages souvent locales prévues à cet effet[342]. Donc, même si les infrastructures conservant ou traitant ces données étaient aux prises avec l'un ou l'autre des risques que nous avons cernés au deuxième chapitre, l'incidence sur certaines des données identifiées comme données d'enseignements se révélerait comme étant superficielle. Dans bien des situations, l'infonuagique apporterait sous plusieurs aspects un avantage à ces données, ne serait-ce que pour leur accessibilité.

Or, les données d'enseignement ne sont pas toutes de cette nature. Certaines des œuvres produites par les étudiants, les chercheurs et les professeurs peuvent être protégées par des droits

---

[340] Groupe consultatif interorganisme en éthique de la recherche, « Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains », Chapitre 3 – Vie privée et confidentialité des données, en ligne : < http://www.ger.ethique.gc.ca/archives/tcps-eptc/docs/TCPSsec03f.pdf>, (consulté le 28 avril 2019).
[341] *Id*. préc., note 142.
[342] Beaucoup d'établissements d'enseignement utilisent des plateformes d'apprentissage, soit librement distribué sous la licence publique générale GNU telle que Moodle (https://moodle.com/) ou encore sous des outils commerciaux comme SharePoint (Microsoft) dans les deux cas, il s'agit d'outil de collaboration dans lequel des informations peuvent être entreposées pour faciliter le partage d'information aux étudiants. Ces deux exemples sont grandement utilisés, mais il existe beaucoup d'autres alternatives à ces solutions.

inhérents à leurs auteurs. Entre autres, dans le cas d'un travail universitaire, l'étudiant est le premier titulaire des droits[343]. En effet, ces travaux constituent des œuvres au sens de l'article 2 de la *Loi sur le droit d'auteur*[344]. Donc sans le consentement explicite de ce dernier, l'ouvrage ne pourrait être traité ou entreposé dans une IaaS. Toutefois, ce raisonnement suggère que le fait de rendre un document accessible, il est aussi « […] communiqué au public, par télécommunication […] »[345]. Ce droit exclusif est d'ailleurs réservé au détenteur du droit d'auteur en vertu de l'article 3 (1) f). Une analyse similaire est faite par certains auteurs concernant les accès aux documents du tribunal.[346] Malgré tout, dans ce cas, il serait également interdit de déposer ces œuvres sur un serveur interne à l'université. Néanmoins, il sera nécessaire de valider la portée des conditions d'utilisation sur les données hébergées ou traités chez un fournisseur externe.

Qui plus est, il est important de rappeler que même des programmes d'ordinateur peu importe le langage de programmation utilisé constitueront également des œuvres littéraires[347] selon cette loi. C'est également l'avis évoqué dans l'« Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le Gouvernement du Québec » :

> « …l'entreposage de documents protégés par droit d'auteur dans le nuage ne sera possible que si les accès à ce document sont interdits aux tiers (ce qui inclus le prestataire de services infonuagiques) ou si le titulaire y consent. » [348] (nos soulignements).

---

[343] COPIBEC, « Saviez-vous que vous détenez les droits d'auteur sur vos travaux scolaires? », 11 Avril 2018, en ligne : <https://www.copibec.ca/fr/nouvelle/165/saviez-vous-que-vous-detenez-les-droits-d-auteur-sur-vos-travaux-scolaires>, (consulté le 28 avril 2019).

[344] *Loi sur le droit d'auteur*, LRC 1985, c C-42., art. 2.

[345] *Id*., art. 3 (1) f).

[346] Voir notamment Karim BENYKHLEF, Jane BAILEY, Jacquelyn BURKELL, et Fabien GÉLINAS, « eAccess to Justice », University of Ottawa Press 2016, page 140, en ligne : <https://commentary.canlii.org/w/canlii/2016CanLIIDocs415.pdf>, (consulté le 28 avril 2019); En effet il est précisé par les auteurs (concernant les accès au document du tribunal) que : « *However, by allowing for eAccess to court documents, courts are not simply making copyright material available, they are effectively communicating them to the public by telecommunication, a right that is reserved to the copyright holder under section 3(1)(f) or the Copyright Act. As one author puts it, courts « have effectively moved from repositories of documents to active publishers. »;* Les auteurs font référence au texte de Karen ELTIS, *Courts, Litigants and the Digital Age: Law, Ethics and Practice*, Toronto, Irwin Law, 2012) par. 54.

[347] *Id.*, Par « œuvre littéraire y sont assimilés les tableaux, les programmes d'ordinateur et les compilations d'œuvres littéraires. (literary work) ».

[348] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 107. Dans cet extrait, les auteurs rappellent également que la notion d'« accès » est utilisée selon le sens de l'Article 2.4 de la *Loi sur le droit d'auteur*.

Toutefois, les travaux étudiants tels que les mémoires, thèses ou tout autre document qui feront l'objet d'un dépôt dans un répertoire où dans un espace institutionnel numérique prévue à cette fin se verront contraint à accorder une certaine permissivité. L'institution responsable de ces exemplaires contraindra leurs auteurs à céder « une licence de diffusion non exclusive, accordant le droit de diffuser et/ou reproduire votre mémoire ou thèse à des fins d'enseignement et de recherche. »[349]. Nous croyons que, comme ces œuvres seront déjà prédisposées à pratiquement tous les risques exogènes aux établissements d'enseignement, la conséquence d'un transfert de ces informations ou de leur traitement dans une infrastructure sous forme de service n'amènera pas de risques supplémentaires.

### 1.1.3 Le traitement des données de gestion en vertu des lois applicables aux organismes publics

Tel que précédemment évoqué, nous scindons les données de gestions en deux catégories; celle de l'établissement[350], ainsi que celle relative aux ressources informationnelles[351]. En ce qui concerne, les données de gestion des établissements d'enseignement, elles seront régies par la *loi sur l'accès*[352]. Cette dernière contraint tout responsable des établissements universitaires du Québec à fournir à la demande un droit d'accès aux documents de son établissement et par le fait même aux infrastructures l'hébergeant[353]. L'utilisation d'une infrastructure sous forme de service pour ces données ne semble pas à première vue bafouer ces droits. Quoi qu'il en soit, il est important d'exclure de ces données de gestion, tous renseignements personnels pouvant y figurer afin de respecter les articles de loi y faisant référence. Nous reviendrons sur cette question dans la section concernant la classification des données. En ce qui concerne les données de gestion des ressources informationnelles, ces dernières contiendront entre autres le reflet de l'infrastructure en utilisation. Par contre, ils pourront aussi contenir des informations sensibles

---

[349] Par exemple, dans le cas de l'Université de Montréal, les étudiants doivent signer une autorisation d'utilisation d'un mémoire ou d'une thèse intégrée au processus de dépôt final de leur travail. Voir à cet effet : Université de Montréal, Secrétariat général, « Politique sur les droits des étudiants et des étudiants de l'Université de Montréal » Recueil Officiel, Numéro 20.9, en ligne : <https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/enseignement/regl20_9-politique-droits-etudiantes-etudiants-universite-de-montreal.pdf>, (consulté le 28 avril 2019).
[350] Voir PREMIÈRE PARTIE, chap. 2, section 2.1.3, par. 1.
[351] *Id*.
[352] *Loi sur l'accès*, art. 6., lequel précise que les universités sont assujetties à la *Loi sur l'accès*.
[353] *Id*., 9.

qui ne devraient pas être divulguées comme des règles de renforcement de la sécurité ou encore les clés associées aux chiffrements utilisés. Encore une fois, les accès accordés en vertu de la *Loi sur l'accès* devront tenir compte de restriction particulière afin de protéger le caractère de ces renseignements sur l'IaaS.

### 1.1.4 Le traitement des données de concernant les étudiants en vertu des lois applicables aux organismes publics

Ces données sont composées principalement de renseignements personnels et confidentiels. Encore ici, la *Loi sur l'accès* a un intérêt prédominant à ces données. Leur traitement sur des infrastructures infonuagiques pourrait paraître non juridiquement raisonnable, mais il en est tout autrement.

En effet, la *Loi sur l'accès* prévoit qu'« [u]n organisme public doit 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. »[354]. Il importe de souligner également que l'établissement d'enseignement 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. […]»[355]. L'utilisation et le traitement des renseignements personnels et confidentiels pourraient donc potentiellement être permis dans une infrastructure sous forme de service dans le cadre d'un contrat engagé par l'université à l'endroit d'un prestataire de service infonuagique.

Nous verrons plus en détail les risques et l'incidence reliés à ce type de données dans la sous-section ci-après portant sur la confidentialité des documents technologiques dans une IaaS.

---

[354] *Loi sur l'accès*, art 63.1.
[355] *Id*., art 67.2.

### 1.1.5 Le traitement des données concernant les membres du personnel en vertu des lois applicables aux organismes publics

Tout comme pour les données détenues sur la clientèle étudiante, de nombreuses données personnelles et confidentielles seront présentes dans les dossiers des membres du personnel. Leurs traitements dans une infrastructure infonuagique apporteront essentiellement les mêmes charges que les données des étudiants. Cela dit, une singularité sera importante à établir, celle de la conservation de ces données. Plusieurs règles de conservation des documents viendront baliser la période pendant laquelle un exemplaire devra être conservé[356]. Nous reviendrons plus précisément sur cette question lorsque nous aborderons en plénitude l'élément de la disponibilité de la triade CID.

Notre examen des lois, règlements et de la doctrine, ne décèle pas de contrainte déterminante empêchant l'exploitation des infrastructures sous forme de service lié directement aux types de données présentes dans le monde universitaire. Nous verrons ci-après si la classification des données représente des obstacles plus importants à son emploi.

## 1.2 Classification des données visées par les lois applicables aux organismes publics

Comme nous l'avons soulevé dans le précédent chapitre, la classification est intrinsèquement liée à l'importance des données soumise à un traitement ou à un entreposage dans une infrastructure sous forme de service. Comme il est mentionné par les auteurs de l'étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec :

> « […] 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

[356] *Id*. préc., note 142.

> d'obligations contractuelles que son hébergement dans le nuage deviendra source de soucis. »[357] (nos soulignements).

Tel qu'il est mentionné, le type de données affectera directement la qualité des mesures de sécurité nécessaires au passage de l'information vers l'infonuagique, de même implicitement, de la responsabilité requise pour leurs traitements. Somme toute, comme le mentionne le Commissariat à la protection de la vie privée du Canada, « la protection de la vie privée n'est pas un obstacle [à l'infonuagique], mais il faut en tenir compte. »[358].

### 1.2.1 Les données publiques visées par les lois applicables aux organismes publics

Comme leur appellation le suggère, les données publiques jouissent d'une liberté quant aux possibilités à être utilisé dans une infrastructure sous forme de service. Leur transfert, la conservation ainsi que leur traitement dans les nuages créer un apport direct à cette classe de données. Notamment, dans la mesure où l'article 9 de la *Loi sur l'accès* donne d'emblée un droit d'accès aux documents d'un organisme public, nous considérons qu'il est juridiquement raisonnable de traiter ces données à même une infrastructure sous forme de service. Tel que soulevé précédemment, l'article 55 de la *Loi sur l'accès* vient préciser 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[…]»[359]. Il est intéressant de noter également que comme l'exprime Éloïse Gratton :

> *« The Quebec legal system has no general exception to the consent requirement for personal information that is publicly available. »*[360].

---

[357] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, résumé, p. V.
[358] CPVPC, « L'infonuagique et la protection de la vie privée », Documents d'orientation du CPVPC, Octobre 2011, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie-et-vie-privee/protection-de-la-vie-privee-en-ligne/infonuagique/02_05_d_51_cc/>.
[359] *Loi sur l'accès*, art. 55.
[360] É. GRATTON, préc., note 160, p. 303.

De plus, l'article 57[361] vient dès lors préciser par exemple que le bottin des employés sera considéré comme public[362]. Nous pouvons aussi extrapoler cet article en y ajoutant, malgré qui n'y paraisse pas intégralement, l'adresse de courrier électronique associé au lieu de travail de l'organisme. Nonobstant cette omission, la LPRPDÉ vient cerner la question de l'adresse électronique[363]. Nous préciserons cet élément dans le prochain chapitre.

L'engouement par les données ouvertes favorise à notre point de vue le passage à l'infonuagique. En effet, comme le mentionne le Conseil du Trésor :

> « Les données ouvertes ont un impact direct sur la transparence de nos institutions, un concept qui est le fondement même de toute démocratie. Les administrations publiques ont tout à gagner à bénéficier de la capacité de surveillance et d'analyse de citoyens et d'experts de la société civile. L'ouverture des données gouvernementales et leur réutilisation stimulent le développement de nouveaux produits et services, contribuant ainsi au développement économique du Québec »[364].

Cette déclaration de la ministre responsable de l'Accès à l'information et de la Réforme des institutions démocratiques, Mme Rita Lc de Santis, ouvre la porte à l'entreposage ainsi qu'au

---

[361] L'article 57 de la *Loi sur l'accès* vient préciser entre autres que :

> « **57.** Les renseignements personnels suivants ont un caractère public:
> 1° 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;
> 2° 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; […] ».

[362] Le bottin n'est qu'à titre d'exemples, car bien plus que seulement ces renseignements sont de caractère public en vertu de la loi. Voir à cet effet *Poisson* c. *Université du Québec à Trois-Rivières*, 1999 QCCQ 10281.

[363] Voir notamment Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner, 2016, 104108 (PCC), dans laquel il est précisé au paragraphe 148 : « *Some email addresses, even in isolation, clearly identify an individual by name and other identifying information, such as their workplace. For example, the information published online contained an email address that purportedly belonged to the Prime Minister of New Zealand, 'john.key@pm.govt.nz'*[…] *However, even where an email address does not identify an individual on its face, it might still identify an individual when combined with other information. For example, it might be possible to conduct an online search to identify the owner of an email address. If that is possible, information associated with the email address is the personal information of that individual.*».

[364] Secrétariat du Conseil du trésor du Québec, « Nouveau portail pour les données ouvertes – Favoriser l'innovation et la diffusion d'information », /CNW Telbec/, 5 avril 2016, en ligne <http://www.fil-information.gouv.qc.ca/Pages/Article.aspx?aiguillage=diffuseurs&type=1&listeDiff=4&idArticle=2404057570>, (consulté le 28 avril 2019).

traitement de ces données dites « ouvertes » puisque les caractéristiques recherchées par le Conseil du Trésor sont au diapason de celles offertes par les infrastructures infonuagiques[365].

### 1.2.2 Les données internes/privées visées par les lois applicables aux organismes publics

Tel que leur dénomination l'entend, les données internes ou privées sont endogènes à chaque établissement d'enseignement. En dépit de cette origine, ils peuvent malgré tout être visés par les prescriptions de la *Loi sur l'accès* s'appliquant aux données publiques précitées. Quoi qu'il en soit, le traitement de ces données sous une infrastructure externe à l'université requiert des mesures de sécurité adéquates à cette classification. Il demeure complexe d'établir clairement l'incidence d'un traitement dans les nuages de ces données puisque nous considérons certaines de ces données comme inextricables[366]. Ce ne sont ni des données publiques pour lesquels les risques seraient moindres, et ce ne sont également pas des données qui une fois traité sur une infrastructure infonuagique pourrait requérir une protection ou des limitations extraordinaires. Notons, par contre que ces données devront être disponible aux intervenants pour qui elles représentent une utilité. Par exemple, comme les universités sont en compétition les unes contre les autres[367], il va de soi que des informations, telles des prévisions d'admission ou des campagnes de publicité, doivent garder une certaine confidentialité. Toutefois, il va de soi qu'une divulgation accidentelle ou l'interception de ces informations par un tiers n'auront pas la même incidence que sur des données confidentielles ou à accès restreint. Nous clarifierons cette question quand nous aborderons la question de disponibilité de la triade CID.

---

[365] Voir PREMIÈRE PARTIE, chapitre 1, section 1.2 Les caractéristiques de l'infonuagique.

[366] Il est précisé à l'article 16 de la *Loi sur l'accès* qu'« organisme public doit classer ses documents de manière à en permettre le repérage. Il doit établir et tenir à jour une liste de classement indiquant l'ordre selon lequel les documents sont classés. Elle doit être suffisamment précise pour faciliter l'exercice du droit d'accès. […]». Bien que pratiquement l'ensemble des types de documents sont listés dans les recueils prévus à cet effet (voir le chapitre sur la classification des données la seconde partie de ce mémoire), nous croyons que le niveau de sécurité nécessaire aux éléments de cette classification sera variable et relatif aux moyens et aux connaissances de ses gardiens.

[367] Julie BARLOW, « La course aux étudiants étrangers », *L'actualité*, 9 février 2018, en ligne : <https://lactualite.com/societe/la-course-aux-etudiants-etrangers/>, (consulté le 28 avril 2019).

### 1.2.3 Les données confidentielles visées par les lois applicables aux organismes publics

Les données confidentielles bénéficient d'une protection en vertu de divers instruments légaux de nature publics permettant de sécuriser leurs maniements sur une infrastructure sous forme de service. Il en va de soi puisque la confidentialité est l'un des éléments de l'obligation de sécurité. Du fait que nous aborderons en profondeur la question de la confidentialité ci-après, nous nous contenterons de rappeler que l'article 25 de la LCCJTI mentionne que :

> « La 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 […] »[368].

Pour les besoins de l'analyse, notons que le commissariat à la protection de la vie privée du Canada viendra tout de même préciser en ce qui a trait à la LPRPDÉ, s'appliquant aux organisations privées[369], qu'il n'est pas interdit de transférer des renseignements personnels à une organisation dans un autre pays aux fins de traitement[370].

Finalement, ajoutons à ce qui a trait au renseignement personnel[371], que selon l'« énoncé d'orientation en infonuagique » pour les entreprises gouvernementale émis par le Conseil du trésor en mai 2016, « Les organismes publics privilégient les solutions infonuagiques lorsque celles-ci offrent un meilleur rapport qualité-prix et permettent une gestion efficace des risques, notamment à l'égard des renseignements personnels. »[372].

Nous ne pourrons donc pas conclure par ce niveau de classification des données que le traitement sur une infrastructure sous forme de service n'est pas envisageable.

---

[368] LCCJTI, art. 25.
[369] La LPRPDÉ définit organisation par « S'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales. ».
[370] CPVPC, préc., note 358.
[371] C.A.I., « Qu'est-ce qu'un renseignement personnel ? », en ligne : <http://www.cai.gouv.qc.ca/citoyens/acces-et-protection-de-vos-renseignements-personnels/quest-ce-quun-renseignement-personnel/>, (consulté le 28 avril 2019).
[372] GOUVERNEMENT DU QUÉBEC, Secrétariat du Conseil du trésor du Québec, « Volet Infrastructures, Énoncés d'orientation en infonuagique, Architecture d'entreprise gouvernementale 3.2 », (Mai 2016), en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG_3_2/Enonces_orientation_infonuagique.pdf>, (consulté le 28 avril 2019).

### 1.2.4 Les données à accès restreint visées par les lois applicables aux organismes publics

À première vue, l'infonuagique laisse présager une aversion aux données à accès restreint. D'entrée de jeu, sans le consentement de toutes les parties concernées, « 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 »[373]. Même si aucune autre tierce partie ne conserve la donnée restreinte, « [u]n organisme public peut refuser de communiquer un secret industriel qui lui appartient. »[374]. Il est donc primordial d'informer les utilisateurs de ces faits avant qu'ils ne joignent une IaaS. Sans quoi, dans des axes de recherches spécifiques, lorsque par exemple, des instances de brevets sont en cours, il sera essentiel de veillez à ce que « l'application de certain article de loi n'ait pas pour effet de révéler une source confidentielle d'information ni le secret industriel d'un tiers. »[375]. Cette disposition n'est pas à prendre à la légère puisque la pérennité de certains brevets pourrait en être affectée, soit par une divulgation accidentelle extraterritoriale, soit par une brève de sécurité liée à un risque infonuagique, ou par un manque de sécurité lors du transfert des données vers les infrastructures sous forme de service. Cette possibilité est envisageable puisque la *Loi sur l'accès* permet à un organisme de communiquer un renseignement à accès restreint[376] « […] 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. »[377].

De plus, les données à accès restreint seront souvent issues de projets universitaires industriels pour lesquels également les lois applicables au secteur privé trouveront application. Nous analyserons ces lois spécifiques dans le prochain chapitre.

---

[373] *Loi sur l'accès*, art. 23.
[374] *Id*., art. 22.
[375] *Id.*, art. 41.2.
[376] *Id.*, art. 41.2.
[377] *Id*., art. 41.2, al. 6.

Ces raisons nous poussent à croire qu'il n'est pas sage de traiter des informations hautement secrètes sur une infrastructure sous forme de service.

Les niveaux de classifications des données numériques influencent grandement l'importance accordée à ceux-ci lors de leur expropriation vers des infrastructures sous forme de service. Plusieurs raisons juridiques sus-citées permettent d'énoncer ces dires, mais il en découle aussi d'une obligation de sécurité. Nous verrons dans les points suivants de quelle règle judiciaire il pourrait être question.

## 1.3 L'obligation de sécurité visant les organismes publics

Ce mémoire ne pourrait être complet et surtout réflexif, sans analyser le côté législatif encadrant la triade CID, et ce, bien que nous ayons déjà soulevé certains des composés de la triade dans des sections de ce chapitre. Comme nous l'avons évoqué, plusieurs lois viennent confiner le traitement des données universitaires dans une IaaS, mais leur portée s'avère tout de même interprétative. Il n'en demeure pas moins que les obligations de sécurité entérinée par le législateur pour les organismes gouvernementaux prennent leurs origines depuis plusieurs documents législatifs. Il est important aussi de préciser que les prestataires de services infonuagiques (canadiens) se baseront sur les lois applicables aux domaines privés et non aux règles habituellement plus rigoureuses imposées aux établissements étatiques[378]. Dès lors que l'on fait affaire avec une institution publique, le prestataire n'aura d'autre choix que d'obtempérer à *la Loi sur l'accès*. C'est au cœur de cette section que nous établirons comment ces obligations balisent l'usage de l'IaaS dans les universités.

### 1.3.1 La confidentialité des données des organismes publics

Comme mentionné auparavant, la principale préoccupation des universités en ce qui a trait à l'infonuagique est la confidentialité de leurs données. Nous avons déjà soulevé quelques articles dans le précédent chapitre faisant mention de cette obligation de sécurité, rappelons notamment l'article 63.1 de *la Loi sur l'accès.*

> « Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués,

[378] J-F DE RICO, préc., note 240.

> 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. »[379] (nos soulignements).

Cet article établit clairement que l'obligation selon laquelle une université[380] doit assurer la protection des renseignements personnels en est une de moyen. Cette intensité attribuable à l'obligation de sécurité semble insuffisante afin d'assurer la confidentialité des données. Judicieusement, l'article 25 de la LCCJTI*,* également déjà cité[381], vient préciser que le degré de protection requis devrait s'arrimer au niveau d'importance de classification des données. Un document public et un document à accès restreint n'auront pas les mêmes prérogatives en ce qui a trait aux mesures de sécurité requise par chacun d'eux. Qui plus est, l'article 26 de la même loi[382], également précédemment cité, vient établir la relation entre la responsabilité bilatérale du propriétaire de l'information ainsi que du prestataire de service.

Il est important de noter que l'infonuagique en générale n'a jusqu'à présent été au cœur d'aucun différend judiciarisé en sol canadien. Nous ne pouvons alors pas statuer à savoir si l'obligation de sécurité en droit des technologies de l'information est une obligation de moyen ou de résultat pour les services infonuagique. Néanmoins, certains auteurs dénotent une mésadaptation au contexte de la sécurité informationnelle tant pour l'obligation de moyen « qui semble trop exigeante envers la victime d'une faille sécuritaire dans le système d'information d'une entreprise »[383] que pour celle de résultat qui « est trop contraignante pour le responsable de la sécurité informationnelle puisqu'elle impose l'implantation d'une sécurité quasi parfaite, ce qui est matériellement, juridiquement et économiquement impossible »[384]. Pour corriger ce tir, Paul-André Crépeau[385] a élaboré deux dérivées : soit l'« obligation de moyen renforcée »[386] et l'« obligation de résultat atténuée »[387]. Ces deux libellés issus d'une intensité obligataire

---

[379] *Loi sur l'accès*, art. 63.1.
[380] Dans cet article, la loi fait référence à tous les organismes publics.
[381] Préc., note 368.
[382] LCCJTI, art. 26.
[383] N. W. VERMEYS, préc., note 75, p. 111.
[384] *Id*., p. 110.
[385] Paul-André CRÉPEAU, *L'intensité de l'obligation juridique*, Cowansville, Éditions Yvons Blais, 1989, p.19.
[386] *Id*., p.16.
[387] *Id*., p.17.

approfondie permettent de mieux répondre aux besoins liés à l'obligation de sécurité. Le niveau le plus conforme aux obligations qui nous concerne serait celle de « l'obligation de moyen renforcée » qui est, selon le professeur Vermeys, celle qui « s'inscrit nécessairement dans l'obligation plus générale de protéger l'information confidentielle concernant ou appartenant à un tiers. »[388].

Cela dit, dans le cas d'un mandat d'implantation d'infrastructure informatique donné à une firme externe il a été établi que :

> « [l]'obligation de résultat est celle en fonction de laquelle le débiteur est tenu de fournir au créancier un résultat précis et déterminé, alors que l'obligation de moyens vise plutôt celle pour la satisfaction de laquelle le débiteur est tenu d'agir avec prudence et diligence en vue d'obtenir le résultat convenu en employant tous les moyens raisonnables, sans toutefois garantir le créancier du résultat. »[389].

À notre point de vue, la nature des obligations, notamment celle traitant de confidentialité devrait en conséquence se retrouver clairement formulée sur le contrat qui sera pris avec le prestataire de service. En effet, comme l'a démontré l'affaire *Caisse Desjardins de Val-Saint-François* c. *GSC Communication*[390]*,* « […] [p]our déterminer si une obligation est de résultat ou de moyens, il faut examiner l'objet du contrat et son caractère aléatoire […] ». La responsabilité contractuelle dont il est question ici est régie par l'article 1458 C.c.Q mentionnant que : « Toute personne a le devoir d'honorer les engagements qu'elle a contractés. […] »[391].

Il nous apparaît donc évident que, lorsqu'il est question d'utiliser une infrastructure externe à l'université, la meilleure protection pour veiller au respect de l'obligation de confidentialité restera l'entente contractuelle puisque :

> « En présence d'un contrat de service, le prestataire de service est tenu d'agir aux mieux des intérêts de son client, avec prudence et diligence. S'il est tenu au résultat, il ne peut se dégager de sa responsabilité qu'en prouvant la force majeure, un manquement du client à ses propres obligations ou la faute d'un tiers. »[392].

---

[388] N. W. VERMEYS, préc., note 383, p.112.
[389] *Caisse Desjardins de Val-Saint-François* c. *GSC Communication inc*., 2018 QCCQ 2125.
[390] *Id*.
[391] C.c.Q., art. 1458.
[392] Mentionnons ici que souvent les prestataires de service infonuagique ont recours à des services hôtes où seront entreposées leurs fermes de serveur, il sera alors fréquent que plusieurs tiers (ou sous-tiers) soient impliqués.

Le législateur a par ailleurs émis des précisions quant aux données à accès restreintes dans l'article 41.2 de la *Loi sur l'accès* :

> « 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. »[393].

Aussi, c'est précisément ce que prévoit l'article 67.2 de la même loi quant aux renseignements personnels :

> « Un 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.
> Dans ce cas, l'organisme public doit:
> 1° confier le mandat ou le contrat par écrit;
> 2° 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. […] »[394] (nos soulignements).

Il importe de souligner que l'université demeurera responsable des atteintes à la confidentialité des données, car c'est à elles de veiller au respect des règles établies pour les services qu'elle contracte telle que mentionné par le secrétariat du Conseil du trésor :

---

[393] *Loi sur l'accès*, art. 41.2.
[394] *Id.*, art. 67.2.

> « De même, les ministères et organismes du GC qui utilisent les services d'informatique en nuage demeurent responsables de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information du GC et des renseignements connexes hébergés par le fournisseur de services d'informatique en nuage. » [395].

Ainsi, dans l'éventualité probable où une université envisagerait l'utilisation d'une IaaS dans une compagnie extérieure du Québec elle devra s'assurer que les renseignements confidentiels « bénéficieront d'une protection équivalant à celle prévue à la présente loi. » tel que mentionné par l'article *70.1 de la Loi sur l'accès*[396]. De cette manière, dans la circonstance où un prestataire de service refuserait des clauses contractuelles afin de parer à l'éventualité des risques liés à l'IaaS, l'impartition de ces services vers l'infonuagique devrait être proscrite ou du moins, comme le soulignent les auteurs Raymond Doray et François Charrette :

> « [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. »[397].

Par ailleurs, dans le cas où une impartition vers un service d'infrastructure sous forme de service serait envisagée, l'utilisation de technique de chiffrement devrait être prise en considération. Bien que le chiffrement puisse pallier certains risques lors du transfert des données[398] vers et depuis l'infrastructure et qu'il en est de même pour les données à l'état inertes[399] à même l'IaaS, celles en traitements causeront certes un obstacle à l'article évoqué. Néanmoins, les services IaaS se peaufinent constamment. Microsoft Azure offre la possibilité

---

[395] SECRETARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : Mise à jour de 2018 », en ligne : <https://www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html>.

[396] L'article 70.1 de la *Loi sur l'accès* mentionne que : « [a]vant 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.
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. ».

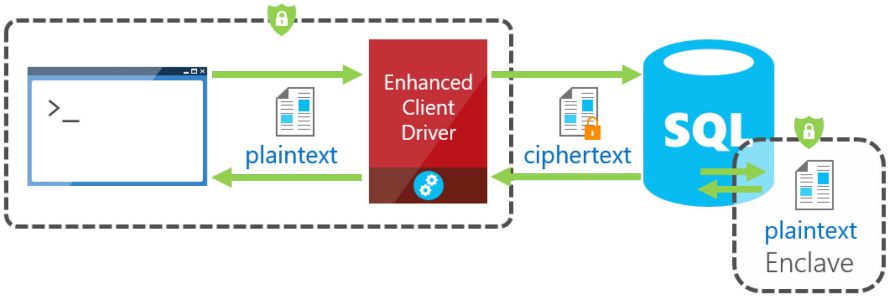
[397] Raymond DORAY et François CHARETTE, *Accès à l'information: loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Éditions Y. Blais, 2001, p. III/70.1-2.

[398] L'article 34 de la LCCJTI requiert l'utilisation d'un niveau approprié au mode de transmission lorsqu'il est question de donnée confidentielle.

[399] D. P. WHELAN, préc., note 259 p. 40.

d'effectuer certaines opérations chiffrées, ces dernières ne pourront alors pas être interceptées ou connues par le prestataire de service[400].

Figure 10. Enclave de chiffrement




Le recours à ces méthodes permettrait de respecter l'ensemble des obligations de confidentialité imputable aux données à caractère confidentiel ou à accès restreint pouvant être traitées dans des IaaS.

Parallèlement, les grandes entreprises offrant des services IaaS ont maintenant des centres de données au Canada et offrent aux entreprises la possibilité d'héberger des données uniquement en sol canadien[401]. Ces offrent comporte parfois des effets néfastes, par exemple « *Google Cloud Plateform* » ne possède qu'une seule région Canadienne[402], cette dernière est située à Montréal. Dans l'éventualité où un désastre affecterait cette région, l'accessibilité aux infrastructures prévues par la loi pourrait en être affectée. Nous étudierons cette question dans la section traitant l'obligation de disponibilité.

Alors, pour s'acquitter des requis de la loi[403] en ce qui a trait à la notion de confidentialité dans une IaaS, les universités, devront avoir recours à des méthodes de chiffrement pour respecter l'ensemble des obligations de confidentialité imputable aux données à caractères confidentielles ou à accès restreint. De plus, dans l'éventualité où un traitement sur ces données est nécessaire et que les opérations lors de ce traitement ne peuvent être effectuées dans des

[400] *Id*., préc., note 235.
[401] Microsoft (Azure), Oracle, Amazon (AWS).
[402] Pour plus d'information, en ligne : <https://cloud.google.com/compute/docs/regions-zones/>, (consulté le 28 avril 2019).
[403] *Loi sur l'Accès*, art. 63.1; LCCJTI, art. 24, art. 25, art. 26.

enclaves sécurisées à chiffrement constant[404], ces opérations devront être effectuées à même l'infrastructure de l'université.

Il importe de rappeler que c'est d'ailleurs ce que mentionne le Conseil du trésor dans l'énoncé d'orientation en infonuagique pour les entreprises gouvernementale : « Le recours à un nuage dédié aux organismes publics est préconisé pour l'hébergement de renseignements personnels et autres données sensibles lorsque l'infonuagique publique ne permet pas de respecter les exigences gouvernementales. » (nos soulignements)[405]. L'énoncé ajout que : « Les renseignements personnels confiés à des prestataires de services infonuagiques doivent être situés au Québec ou bénéficier d'un niveau de protection jugé équivalent conformément au cadre juridique québécois. »[406].

### 1.3.2 L'intégrité des données des organismes publics

L'importance de l'obligation du maintien à l'intégrité en droits des TI est issue de la LCCJTI[407]. En effet, la notion d'intégrité est mentionnée près de 40 fois dans ce texte de loi. Il s'agit du deuxième élément de la triade, mais il demeure tout aussi déterminant que ses analogues dans le processus décisionnel d'impartition d'une infrastructure informatique universitaire vers une IaaS. Nous avons déjà vu dans la première partie de ce mémoire l'importance de l'intégrité reliée à l'utilisation d'une infrastructure sous forme de service, nous verrons maintenant l'obligation d'intégrité réelle issue du cadre législatif en vigueur. Comme nous l'avons vu, l'article 25[408] énonce l'obligation qui incombe au responsable de l'accès de mettre en place les mesures de sécurité nécessaires pour préserver la confidentialité, et l'article 26 encadre l'éventualité où le document est confié à un prestataire de service :

> « Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la

[404] *Id*., préc., note 235.
[405] C.A.I., préc., note 372.
[406] *Id*.
[407] Évidemment, aussi du C.c.Q. qui a été modifié par la LCCJTI.
[408] LCCJTI, art. 25.

> confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. […] »[409] (nos soulignements).

Certains auteurs[410] ont attiré précédemment l'attention sur la « *garde du document* ». Cette « *garde* » est essentiellement « *plus rigoureuse que la seule obligation du respect de l'intégrité* »[411] et devrait donc être interprétée comme requérant une obligation de chiffrement.

Toutefois, à quoi bon mettre en place des mesures de sécurité pour préserver la confidentialité si l'intégrité des données n'est pas certifiée ? Ces deux éléments de la triade sont très complémentaires, et l'intégrité des données aura elle aussi une très grande répercussion sur l'utilisation d'une IaaS dans les universités. L'intégrité sera préservée si des mesures de sécurité permettent de protéger le document tout au long de son cycle de vie :

> « 6. 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 <u>la stabilité et la pérennité</u> voulue.
>
> L'intégrité du document doit être maintenue <u>au cours de son cycle de vie</u>, 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.
>
> Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son <u>cycle de vie</u>. »[412] (nos soulignements).

Malgré que l'article 6 de la LCCJTI ne fait pas de mention précise de la notion de « traitement » qui est celle qui est interpellée entre autres par une utilisation dans une IaaS, puisqu'il est question de tout au long du « cours de cycle de vie » nous établirons ce fait comme implicite.

Les notions de « pérennité » et de « cycle de vie » mentionnées par cet article doivent entraîner les universités à spécifier des mesures particulières à prendre contractuellement pour veuillez à ce que les procédures de sauvegarde, d'archivages et de destruction des services et des données contenues dans l'infrastructure respectent le cadre légal mis en place, notamment

---

[409] LCCJTI, art. 26.
[410] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montréal, Éditions Thémis, 2010.
[411] *Id.*
[412] *Id.* préc., note 242.

pour les renseignements personnels,[413] mais également pour répondre aux clauses contractuelles effectives avec les partenaires industriels et commerciaux des universités et des centres de recherches. Tout compte fait, comme l'a mentionné la commission de l'éthique, de la science et de la technologie : « moins longtemps les données sont conservées, moins les risques de détournement d'usage sont grands »[414].

À l'évidence, comme nous l'avons démontré dans l'analyse des risques associés à l'utilisation d'une infrastructure sous forme de service[415], quoique très important, l'intégrité est l'élément le moins névralgique, puisqu'il est facilement vérifiable. En effet, la présence des métadonnées permet de certifier l'intégrité d'un document[416], mais comment pouvons-nous vérifier ces propriétés dans une IaaS ? Tel que nous l'avons constaté, un seul risque dans le précédent chapitre était lié exclusivement à l'obligation d'intégrité, il s'agit de « la perte, la compromission ou l'inexistence des journaux d'opération et de sécurité ». En l'occurrence, afin d'apprécier l'intégrité des données traitées dans une IaaS l'enregistrement événementiel de ses états doit être mis en place par les administrateurs. Heureusement, des fonctions de vérification d'intégrité sont incorporées dans les actifs information, les processus opérationnels, la logique des logiciels ainsi que dans le matériel utilisé au sein de l'infrastructure[417]. Encore faut-il qu'elle soit scrutée pour constater les irrégularités.

Rappelons que la LCCJTI prévoit également que :

> « Toute 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. »[418] (nos soulignements).

Comme nous pouvons le constater, la disponibilité d'un document et bien entendu la disponibilité d'une infrastructure sous forme de service sera tout à fait inutile si son état n'est pas intègre.

---

[413] *Loi sur l'accès,* art. 63.1.
[414] COMMISSION DE L'ÉTHIQUE, DE LA SCIENCE ET DE LA TECHNOLOGIE, « Viser un juste équilibre, Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité », Avis adopté à la 34e réunion de la Commission, Gouvernement du Québec, 12 février 2008, p. xxiv.
[415] Voir Annexe 1, Analyse de Risque.
[416] *Sécurité des Deux-Rives ltée* c. *Groupe Meridian construction restauration inc.,* 2013 QCCQ 1301, par. 51.
[417] *Id.*, préc., note 395.
[418] LCCJTI, art. 19.

Dans le but d'assurer l'intégrité, l'article 15 de la LCCJTI prévoit que :

> « […] le procédé employé doit présenter des garanties suffisamment sérieuses pour établir le fait qu'elle comporte la même information que le document source.
> Il est tenu compte dans l'appréciation de l'intégrité de la copie des circonstances dans lesquelles elle a été effectuée de façon systématique et sans lacunes ou conformément à un procédé qui s'appuie sur des normes ou standards techniques approuvés par un organisme reconnu visé à l'article 68. »[419].

Cette disposition, quoique prévue pour les données, est à notre point de vue transposable à une infrastructure.

Bien entendu, nous retrouverons citées à l'article 68 évoqué dans ce dernier article différentes sources dont nous avons tirés ressources pour la rédaction de ce mémoire.

> « […]
> 1° la Commission électrotechnique internationale (CEI), l'Organisation internationale de normalisation (ISO) ou l'Union internationale des télécommunications (UIT) ;
> 2° le Conseil canadien des normes et ses organismes accrédités ;
> 3° le Bureau de normalisation du Québec. »[420].

Évidemment, tous les grands fournisseurs offrant des infrastructures sous forme de services répondant aux besoins universitaires, par exemple Microsoft, mettront à la disposition des utilisateurs actuels ou futurs les rapports d'audit dans le but de vérifier les conformités techniques et les exigences de contrôle afin de se judiciariser[421].

Nous l'avons aussi évoqué, l'intégrité se doit aussi d'être préservée lors de la transmission de l'information. Dans le cas où une université viendrait à scinder une part de ses infrastructures locales vers une IaaS, la quantité d'information à échanger avec le tiers fournisseur serait telle qu'elle devra utiliser des moyens efficaces. Certains de ces procédés sont mentionnés à l'article 30 de la LCCJTI :

---

[419] *Id*., art. 15.
[420] *Id.,* art. 68.
[421] Voir à cet effet, Microsoft Corporation, « Rapports d'audit », en ligne : <https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=e9db0154-b5c6-4570-9c63-c0c20b3519bc&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports>, (consulté le 28 avril 2019).

> « […] 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. »[422].

Finalement, malgré qu'il soit possible d'entériner l'effort offert par les fournisseurs de services infonuagiques pour faire référence à l'obligation d'intégrité, nous recommandons tout de même d'utiliser, du moins ici, les services du Centre de Services Partagés Québec[423] qui sont mandatés afin de cibler les fournisseurs conformes aux besoins des organismes provinciaux.

### 1.3.3 La disponibilité des données des organismes publics

La dernière obligation de sécurité de la triade CID, mais non la moindre, est la disponibilité. Rappelons que l'obligation de disponibilité pour les organismes publics regroupe deux principaux objectifs : Le premier étant que « Toute personne qui en fait la demande a droit d'accès aux documents d'un organisme public. »[424]. Quant au second, il dispose que la disponibilité des données doit être possible lorsqu'elle est nécessaire aux personnes devant y avoir accès dans l'exercice de leurs fonctions[425].

Aux fins d'assurer l'accessibilité ainsi que le droit d'accès à l'information, tel que prescrit par l'article 10 de la *Loi sur l'accès*, il ne sera bien entendu pas possible, ou du moins, vide de sens, de permettre d'accéder «[…] à un document […] sur place pendant les heures habituelles de travail ou à distance. »[426]. Cet article de loi prévoit tout de même qu'« [à] la demande du requérant, un document informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible. »[427]. Néanmoins, le passage vers une IaaS pourrait potentiellement compliquer ces accès puisque les documents non publiquement affichés et

---

[422] LCCJTI, art. 30.
[423] Centre de service partagés Québec, (ci-après « CSPQ ») : « Le CSPQ offre des services partagés de qualité pour générer des économies de temps et d'argent pour le gouvernement du Québec et ainsi contribuer à assurer la pérennité des services aux citoyens. », voir à cet effet : en ligne : <https://www.cspq.gouv.qc.ca/>, (consulté le 28 avril 2019).
[424] *Loi sur l'accès*, art. 9.
[425] *Id.*, art. 62. Cet article fait cette mention à l'égard des renseignements personnels, mais il va de soi que nous pourrons converger ces arguments de disponibilité dans un cadre plus large.
[426] *Loi sur l'accès*, art. 10.
[427] *Id*.

accessibles depuis le site web de l'institution ne seront fort probablement inaccessibles autrement que par l'entremise d'accès informatiques restreints.

Pour être disponible, l'infrastructure se doit d'être opérante, notamment afin de répondre au besoin de confidentialité des organismes gouvernementaux. À cette fin, les fournisseurs de service infonuagique ont débuté l'établissement de centre de données et de traitement en sol canadien. L'offre, quoiqu'intéressante d'un point de vue de la protection des renseignements personnels et des informations confidentielles, rend vulnérable la disponibilité des données. Cela va sans dire qu'une concentration des données ou des infrastructures dans un même territoire affaiblit la capacité à atténuer le risque[428]. Nous avons soulevé le cas de Google Cloud Platform qui était dans une situation bien limitative pour répondre au besoin de disponibilité des universités.

Il importe également de rappeler que la notion de disponibilité doit être limitée dans le temps. Encore particulièrement en ce qui a trait aux renseignements personnels pouvant être conservés dans les établissements d'enseignement. À cet effet la loi dicte que :

> « Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire, sous réserve de la *Loi sur les archives* (chapitre A-21.1) ou du *Code des professions* (chapitre C-26). »[429].

Ce requis en termes de limitation doit toutefois être cohérent avec les obligations définies par la *Loi sur les archives* qui pointe vers le recueil des règles de conservation des documents des établissements universitaires québécois[430]. Cette dichotomie est importante à souligner, mais elle pourrait possiblement faire l'objet d'un mémoire à elle seule. Rappelons néanmoins que les règles de conservation du CREPUQ sont strictes et clairement établies, contrairement au délai supposé des prestataires de service infonuagique[431].

Nous avons soulevé la loi comme outil, mais aussi, ultimement le contrat établi avec le prestataire de service est un des mécanismes prévus par le législateur permettant d'assurer du

---

[428] Voir notamment, l'Analyse de risque en Annexe 1, R.21 Catastrophe Naturelle.
[429] *Loi sur l'accès*, art. 73.
[430] *Id*. préc., note 142.
[431] Nous avons constaté que cette période peut s'étendre jusqu'à 6 mois dans certain cas. Voir notamment : Google cloud Documentation, « suppression des données sur GCP », 20 février 2019, en ligne <https://cloud.google.com/security/deletion/>, (consulté le 28 avril 2019).

moins un taux minimum ou idéalement une disponibilité continue des services infonuagiques. Parfois, le contrat, aussi détaillé soit-il, pourrait ne pas suffire à assurer l'obligation de disponibilité. Notamment, lorsque le premier risque défini en annexe, soit la « Fermeture ou le changement du service infonuagique », affecte l'un des tiers. La justice a d'ailleurs dû réfléchir et prendre décision sur cette question dans le cas *Oracle Canada* c. *Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île de Montréal*[432]. Ce litige se rapporte à l'interprétation d'un contrat signé à l'origine par la société Taléo avant son acquisition par Oracle pour la fourniture de services infonuagiques.

Dans ce cas, des conditions supplémentaires ont été incorporées par renvoi vers les conditions de la convention de services infonuagique Oracle disponible sur le site Internet de l'appelante. Cette convention « remplace toutes les autres conventions antérieures et se trouve, par conséquent à abroger la disposition de renouvellement automatique […] »[433]. Ces changements ont eu pour effet de produire un désaccord à propos des modalités de facturation pour le service qui aurait pu mettre en péril (la cause ne fait pas de mention expressément à cet effet) l'accès aux services infonuagique hébergé chez le prestataire.

> « *As of July 2016, a disagreement emerged between the parties regarding the interpretation of their agreement* […] *and in particular, how billing is calculated.* »[434].

Le juge Peacock de la cour supérieure s'appuyant sur l'article 1435 du C.c.Q., estime que la nouvelle convention, n'étant pas raisonnablement accessible, ne s'appliquerait pas. L'appel rejeté est venu confirmer ses dires.

Néanmoins, pour pallier ces risques, le choix du prestataire d'infrastructure infonuagique devrait tenir compte d'un plan de continuité des services advenant un différend jusqu'à la résolution du conflit.

---

[432] *Oracle Canada* c. *Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île de Montréal*, 2018 QCCA 1011.
[433] *Id*.
[434] *Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île-de-Montréal* c. *Oracle Canada*, 2017 QCCS 6377.

Tout comme dans la section sur l'obligation d'intégrité, le principe de disponibilité de l'IaaS est couvert par l'article 19 de la LCCJTI. Rappelons que celui-ci mentionne:

> « Toute 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. »[435].

Aux fins du présent mémoire, le matériel qui permet de rendre accessibles les documents universitaires est bien entendu l'infrastructure infonuagique.

La question de l'intelligibilité est également soulevée à l'article susmentionné de la LCCJTI. Cette caractéristique apparaissant aussi à l'article 23 de la même loi, constitue un renvoi aux technologies employées pour la conservation ou la transmission de l'information. Advenant que des techniques de chiffrement soient à l'emploi à même l'infrastructure, certains cas pourraient nécessiter la rémission des outils nécessaires afin de permettre la lisibilité des données.

Le mandat de perquisition ou un jugement pourrait être l'un de ces cas. Par exemple, dans *Digital Shape Technologies Inc.* c. *Comte*[436] il a été demandé :

> «[…] aux défendeurs de fournir tous comptes d'utilisateurs et/ou mots de passes pour accéder aux données de leurs appareils électroniques, soit le compte d'utilisateur et mot de passe des systèmes d'exploitation, les mots de passe de déchiffrement de document, de disque dur, ou de clé USB, les mots de passe pour téléphone portable et d'applications »[437].

Dans le même jugement préliminaire, la juge Christine Baudouin ne croit pas abusif, sans toutefois accorder l'accès de permettre aux défendeurs :

> « […] de donner accès à tous leurs comptes de messagerie électronique et comptes infonuagiques à la firme d'experts KPMG en leur procurant leurs noms d'utilisateur et mots de passe à jour; »[438] [KPMG ici, était chargé d'analyser toutes les données pour le compte de la partie demanderesse].

Elle laisse alors le soin au juge du fond d'ordonner la divulgation si la preuve l'exige :

---

[435] LCCJTI, art. 19.
[436] *Digital Shape Technologies inc*. c. *Comte* 2018 QCCS 1199.
[437] *Id*. par. 20.
[438] *Id*. par. 21.

> « [53] Toutefois, il est possible que le juge du fond après avoir entendu l'ensemble de la preuve et ayant une vision globale de l'ensemble du dossier, et du comportement allégué de la demanderesse puisse constater le caractère inutile, abusif ou excessif des procédures, incluant la demande en préservation et divulgation de la preuve comme partie intégrante du dossier. Il sera certes mieux placé alors, pour sanctionner a postériori l'utilisation déraisonnable de la procédure le cas échéant »[439].

Nous pouvons dès lors conclure que, si une méthode de chiffrement est utilisée sur une infrastructure sous forme de service, dans le cas d'un litige, il sera possible pour les autorités compétentes de saisir les données nécessaires à l'exécution d'un jugement.

Si le droit applicable aux organismes publics permet de déterminer certaines balises quant à la possibilité du passage vers l'utilisation d'une infrastructure sous forme de service dans les universités, d'autres documents comme les politiques, les directives ainsi que des procédures de fonctionnements internes des universités pourront aider à cerner les possibilités d'impartition.

L'évaluation et l'acceptabilité des risques liés à l'utilisation d'une IaaS au sein des universités sont cruciales pour faire une transition efficace et sécuritaire. Force est d'admettre que nous vivons une judiciarisation croissante de l'infonuagique. Cependant, la mise en place d'une IaaS demeure à notre point de vue ambigu, puisque peu ou pas d'organisme public ont été impliqués dans des problématiques juridiques sur la question.

Pour conclure ce chapitre, nous devons mentionner que les incidences juridiques en lien avec le droit applicable aux organismes publics influençant l'utilisation des IaaS sont en partie encadrées par la mise place d'une stratégie infonuagique gouvernementale émanent du *règlement sur les contrats du Protecteur du citoyen*[440] au sujet de l'acquisition de biens ou de services infonuagiques voulant que :

> « Un contrat pour l'acquisition de biens ou de services infonuagiques peut être conclu de gré à gré avec un fournisseur ou un prestataire de services qui, à la suite d'un appel d'intérêt effectué par le Centre de services partagés du Québec, a conclu une entente-cadre avec celui-ci en application du D. 923-2015, 2015-10-

[439] *Id*. par. 53.
[440] *Règlement sur les contrats du Protecteur du citoyen*, RLRQ c P-32, r 2.

> 28 et ses modifications, le cas échéant, dans la mesure où les conditions suivantes sont remplies:
> 1° le contrat porte sur un bien ou sur la prestation d'un service visé par l'entente-cadre;
> 2° la durée du contrat n'excède pas 3 ans, incluant tout renouvellement;
> 3° le fournisseur ou le prestataire de services retenu par l'organisme public est celui qui lui offre le bien ou le service le plus avantageux.
> Pour déterminer le bien ou le service le plus avantageux, le Protecteur du citoyen se fonde:
> 1° soit uniquement sur le prix;
> 2° soit, après autorisation de son dirigeant, sur un ou plusieurs autres critères en lien avec l'objet du contrat, telles la compatibilité technologique, l'accessibilité des biens ou des services, la performance et l'assistance technique. ».[441]

Dans le prochain chapitre, il sera question des liens de l'infonuagique avec les lois spécifiques au secteur privé dans les universités. Nous verrons alors si une inflexion surviendra quant à la possibilité de recourir à l'utilisation d'une infrastructure sous forme de service dans le milieu universitaire.

[441] *Id*., préc., note 440, section IV article 69.

# Chapitre II. L'obligation découlant des lois spécifiques au secteur privé.

Dans la foulée du précédent chapitre, nous poursuivons notre réflexion quant à l'application des lois relative au secteur privé. En effet, dans certains cas, l'université prendra part à une relation tripartite, incluant un organisme tiers issu du secteur privé, voire même plus d'un.

Mentionnons tout de suite que, tout comme il a été indiqué précédemment dans ce mémoire, le domaine universitaire au cœur de notre réflexion implique des acteurs industriels. Ces protagonistes pourront prendre part dans différents types de collaboration, par exemple[442] :

- Recherche contractuelle
- Recherche collaborative (par la participation à un partenariat ou à un programme de recherche)
- Stages en entreprise
- Association avec un institut, un centre ou une Chaire de recherche (recherche commanditée)
- Entente d'utilisation de licence
- Essais (in situ ou in vitro)
- Projets incubateurs de démarrage d'entreprise
- Mentorat
- Consultation/échange d'information de part et d'autre
- Formations / cours de part et d'autre

En revanche, les règles de droit visant les entreprises privées ne cibleront que quelques types et catégories de données. C'est pourquoi, dans ce chapitre, nous ne reprendrons pas chacun des points du chapitre précédent en relation avec le droit s'appliquant au secteur public. Nous traiterons sans équivoque des données de recherche, mais également des données d'enseignements, des données de gestions ainsi que des données concernant les étudiants et les membres du personnel. Nous devrons aussi établir des liens avec les niveaux de classifications de données auxquels nous avons préalablement fait référence. De plus, nous ne pouvons nous

[442] Certains de ces types de collaborations sont tirés d'un sondage de la Chambre de commerce du Montréal Métropolitain effectué en 2012 concernant la « collaboration universités-entreprises : le regard des centres et chaires de recherche », en ligne : <https://www.ccmm.ca/documents/pdf/RDVS-Savoir2012_fr.pdf>, (consulté le 28 avril 2019).

abstenir de rétablir les faits attribuables à ces fondements relatifs au droit applicable aux entreprises et organismes du secteur privé pour le volet de l'obligation de sécurité. Pour ce faire, nous utiliserons la triade à laquelle nous faisons référence depuis le commencement de notre recherche soit, à nouveau, la confidentialité, l'intégrité et la disponibilité attribuable aux services infonuagiques, mais cette fois-ci pour les règles relevant du secteur privé.

## 2.1 Les types de données liés aux activités impliquant le secteur privé

Comme plusieurs activités académiques ou de recherche visent l'établissement de partenariat avec les entreprises privées, les universités se doivent de prendre plusieurs précautions quand il est question d'impartir leurs infrastructures vers un tiers prodiguant des services infonuagiques. Dans de tels cas, le cadre juridique applicable inclurait encore une fois la LCCJTI, mais également par la LPRPSP, et ultimement par la LPRPDÉ lorsque les IaaS ou l'un de leurs partenaires procèderont à des hébergements transfrontaliers. À ce propos, l'auteur Jean-François De Rico, rappelle que

> « Le Décret d'exclusion visant des organisations de la province de Québec (DORS/2003-374) adopté en vertu de l'article 26(2)b) de la LPRPDE écarte l'application de la partie 1 de la LPRPDE « à l'égard de la collecte, de l'utilisation et de la communication de renseignements personnels qui s'effectuent à l'intérieur de la province de Québec ». Dans les Lignes directrices sur le traitement transfrontalier des données personnelles, le Commissariat à la protection de la vie privée du Canada mentionne expressément « les organisations dont les activités commerciales dans une province ne sont pas assujetties à la LPRPDE doivent savoir que les transferts transfrontaliers le sont ». »[443].

[443] J-F DE RICO, préc., note 240, p. 4.

### 2.1.1 Les données de recherche visées par les lois spécifiques au secteur privé

Comme nous l'avons vu dans le chapitre précédent, les règles de droit applicables aux organisations publiques, pour ce qui a trait aux données reliées à la recherche universitaire, posent certains obstacles à une impartition dans une IaaS. Du moins, lorsque cette impartition est destinée à être utilisée dans un modèle de type public. En effet, rappelons que les enjeux liés à la recherche, tel que nous l'avons soulevé jusqu'ici, relèvent de la question de la propriété intellectuelle.

Puisque les différentes collaborations citées d'entrée de jeu dans ce chapitre sont en grande partie associées à des activités de recherches en lien avec des entreprises privées, quelle sera l'incidence des règles de droit de ce secteur sur leurs traitements en IaaS?

Mentionnons d'emblée que ce ne sont pas tant les types de données qui seront ciblés par la loi, mais plutôt leurs classifications. Néanmoins, les universités ne peuvent laisser pour contre ces investissements sans mettre en place des règlements, directives, politiques et procédures pour restreindre les ambiguïtés pouvant surgir à l'issue des partenariats entre des chercheurs et une entreprise privée. Par exemple, l'Université de Montréal a mis en place une liste exhaustive de politiques attribuables à la recherche, telles que[444] :

- Politique sur la recherche avec des êtres humains[445]
- Politique de l'Université de Montréal sur les brevets d'invention : Principes, Règlements et procédure[446]
- Politique institutionnelle sur l'utilisation d'animaux en recherche et en enseignement[447]

---

[444] Université de Montréal, Secrétariat général, « Règlements, directives, politiques et procédures reliées à la rechercher à l'Université de Montréal », en ligne : <https://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/#recherche>, (consulté le 28 avril 2019).

[445] *Id*., « *Politique sur la Recherche avec des êtres humains* » Numéro 60.1, 1 Novembre 2004, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_1-politique-recherche-avec-etres-humains.pdf >, (consulté le 28 avril 2019).

[446] *Id*., « *Politique de l'Université de Montréal sur les brevets d'invention : Principes, Règlements et procédure* » Numéro 60.2, 18 Septembre 1978, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_2-politique-universite-de-montreal-brevets-invention-principes-reglements-procedure.pdf>, (consulté le 28 avril 2019).

[447] *Id*., « *Politique institutionnelle sur l'utilisation d'animaux en recherche et en enseignement* » Numéro 60.3, 3 Novembre 2003, Recueil Officiel, en ligne : <

- Politique de l'Université de Montréal sur le droit de publication : Énoncé de principes[448]
- Principes concernant l'utilisation des revenus provenant des fonds de recherche[449]
- Politique de diffusion des résultats de la recherche[450]
- Éléments d'une politique de développement de la recherche à l'Université[451]
- Politique de l'Université de Montréal sur les services à la collectivité[452]
- Principes et procédures relatifs à la création, l'évaluation et l'abolition de centres de recherche à l'Université de Montréal[453]
- Politique de l'Université de Montréal sur la probité intellectuelle en recherche[454]
- Procédures d'examen des allégations d'inconduite scientifique visant les professeurs et chercheurs de l'Université ayant obtenu une subvention ou un contrat de recherche d'organismes relevant du gouvernement fédéral des États-Unis[455]

---

https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_3-politique-institutionnelle-utilisation-animaux-recherche-enseignement.pdf>, (consulté le 28 avril 2019).

[448] Université de Montréal, Secrétariat général, « *Politique de l'Université de Montréal sur le droit de publication : Énoncé de principes* » Numéro 60.4, 23 février 1981, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_4-politique-universite-de-montreal-droit-publication-enonce-principes.pdf >, (consulté le 28 avril 2019).

[449] *Id*., « *Principes concernant l'utilisation des revenus provenant des fonds de recherche* » Numéro 60.5, 23 février 1981, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_5-principes-utilisation-revenus-fonds-recherche.pdf >, (consulté le 28 avril 2019).

[450] *Id.*, « *Politique de diffusion des résultats de la recherche* » Numéro 60.6, 9 mai 1984, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_6-politique-diffusion-resultats-recherche.pdf >, (consulté le 28 avril 2019).

[451] *Id.*, « *Éléments d'une politique de développement de la recherche à l'Université* » Numéro 60.7, 9 mai 1984, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_7-elements-politique-developpement-recherche-universite.pdf >, (consulté le 28 avril 2019).

[452] *Id.*, « *Politique de l'Université de Montréal sur les services à la collectivité (voir article 30.4)* » Numéro 60.9, 28 mai 1985, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_9-politique-universite-de-montreal-services-collectivite.pdf>, (consulté le 28 avril 2019).

[453] *Id.*, « *Principes et procédures relatifs à la création, l'évaluation et l'abolition de centres de recherche à l'Université de Montréal* » Numéro 60.10, 23 février 1981, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_10-principes-procedures-creation-evaluation-abolition-centres-recherche-universite-de-montreal.pdf>, (consulté le 28 avril 2019).

[454] *Id.*, « *Politique de l'Université de Montréal sur la probité intellectuelle en recherche* » Numéro 60.11, 29 Mars 2016, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/Rech60_11-Politique_probite_intellectuelle_recherche.pdf >, (consulté le 28 avril 2019).

[455] *Id.*, « *Procédures d'examen des allégations d'inconduite scientifique visant les professeurs et chercheurs de l'Université ayant obtenu une subvention ou un contrat de recherche d'organismes relevant du gouvernement fédéral des États-Unis* » Numéro 60.11.1, 15 Décembre 2003, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_11_1-procedures-examen-allegations-inconduite.pdf>, (consulté le 28 avril 2019).

- Politique des frais indirects en recherche de l'Université de Montréal[456]
- Politique de l'Université de Montréal sur la propriété intellectuelle[457]
- Création de groupes de recherche (guide)[458]

L'examen de ces politiques nous permet de constater que les universités ou leurs filiales de recherche[459], qui traiteront des données de part et d'autre, auront une obligation légale de protéger les renseignements personnels qu'ils pourraient détenir ou traiter en vertu de la LPRPSP[460]. En effet, si les obligations ciblant les institutions gouvernementales sont habituellement assujetties à la *Loi sur l'accès*, il est fort probable que des données détenues ou utilisées aient des liens avec des entreprises privées. Ajoutons aussi que, tel que le mentionne le professeur Pierre Trudel en ce qui a trait à la notion d'entreprise définit à l'article 1525 al. 3[461] du C.c.Q. :

> « […] l'exploitation d'une entreprise suppose l'exercice d'une activité économique organisée, que cette activité soit ou non à caractère commercial. Cette activité peut consister dans la production ou la réalisation de biens. Elle peut aussi concerner l'administration, l'aliénation de biens ou la prestation de services. Le champ d'application de la Loi sur la protection des renseignements personnels dans le secteur privé est ainsi très large […] »[462].

---

[456] *Id*., « *Politique des frais indirects en recherche de l'Université de Montréal* » Numéro 60.12, 20 Décembre 1994, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_12-politique-frais-indirects-recherche-universite-de-montreal.pdf >, (consulté le 28 avril 2019).

[457] *Id*., « *Politique de l'Université de Montréal sur la propriété intellectuelle* » Numéro 60.13, 12 Décembre 1994, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_13-politique-universite-de-montreal-propriete-intellectuelle.pdf >, (consulté le 28 avril 2019).

[458] *Id*., « *Création de groupes de recherche (guide)* » Numéro 60.14, Septembre 2012, Recueil Officiel, en ligne : < https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/doc_officiels/reglements/recherche/rech60_14-creation-groupes-recherche-guide.pdf >, (consulté le 28 avril 2019).

[459] *Id*., La recherche universitaire sur plusieurs formes : Centre, regroupement, groupe, équipe, etc.

[460] *Id*., préc., note 445.; ou encore : Université Laval, « Directive relative à la gestion des renseignements personnels et du matériel Biologique recueillis dans le cadre de projets de recherche impliquant des sujets humains », 20 Avril 2005, en ligne : <https://www.ulaval.ca/fileadmin/ulaval_ca/Images/recherche/Documents/Politiques/Directives_bd_renseignement_personnels_CA.pdf>, (consulté le 28 avril 2019).

[461] L'article 1525 al. 3 du C.c.Q. dispose que: « *Constitue l'exploitation d'une entreprise l'exercice, par une ou plusieurs personnes, d'une activité économique organisée, qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services. ».*

[462] Pierre TRUDEL et France ABRAN, « Guide sur la protection de la vie privée dans les services de courrier électronique en site web », Chaire L.R. Wilson sur le deroit des TI et du Commerce Électronique, CRDP. 24

À la lumière de cette réflexion, nous sommes d'avis que les universités sont des organismes publics, mais leur démembrement, que sont les instituts, centres ou groupe de recherche universitaire opèrent tels que des entreprises privées. Évidemment, pour être désignés comme une entreprise privée, les centres devraient avoir une personnalité juridique, ce n'est habituellement pas le cas, néanmoins, il existe des exceptions.[463]

Suite à ceci, mentionnons que l'article 10 de la LPRPSP précise que :

> « Toute personne qui exploite une entreprise doit 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. »[464].

Indubitablement, cette obligation est pratiquement identique à celle de l'article 63.1 de la *Loi sur l'accès*[465] précédemment étudié s'appliquant déjà aux organismes publics et ciblant également ceux-ci.

La LPRPSP intègre aussi des mentions afin de faciliter la conduite de la recherche, lorsqu'autorisée par la Commission d'accès à l'information, notamment par l'article 18 dont l'alinéa 8 édicte :

> « Une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel contenu dans un dossier qu'elle détient sur autrui :
>
> […]
>
> 8° à une personne qui est autorisée à utiliser ces renseignent à des fins d'étude, de recherche ou de statistique conformément à l'article 21 ou à une personne qui est autorisée conformément à l'article 21.1;
>
> […]»[466].

---

octobre 2000, en ligne : <http://pierretrudel.chairelrwilson.ca/pdf/courrier_site_web.pdf>, (consulté le 28 avril 2019).

[463] Par exemple, le CRDP n'a pas de personnalité juridique, mais IVADO si, voir Registre des entreprises du Québec, opère sous le nom d'IVADO LABS.

[464] LPRPSP, art. 10.

[465] L'article 63.1 *de la Loi sur l'accès*, prévoit qu'« Un organisme public doit 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. ».

[466] LPRPSP, art. 18.

Un résultat semblable se produit à la lecture du troisième alinéa de l'article 18.2 de la même loi, qui se lit comme suit :

> « […] les renseignements qui y sont visés peuvent être communiqués, sans le consentement de la personne concernée, à une personne à des fins de recherche avant l'expiration des délais prévus, si les documents ne sont pas structurés de façon à être retrouvés par référence au nom d'une personne ou à un signe ou symbole propre à celle-ci et s'il n'y a pas de moyen pour repérer ces renseignements à partir d'une telle référence. Cette personne doit respecter le caractère confidentiel des renseignements personnels pendant le délai où ils ne peuvent être communiqués sans le consentement de la personne concernée. »[467]. (nos soulignements).

Ces permissions semblent autoriser, du moins pour des cas de recherches universitaires, l'utilisation et le traitement de renseignements personnels dans une IaaS sous certaines conditions particulières, et ce, tout comme cela aurait été possible dans un centre de recherche utilisant des systèmes informatiques conventionnels. Il demeure essentiel de rappeler que, comme le mentionne le texte de l'article 18, pour se prévaloir d'un tel droit « La personne qui exploite une entreprise doit inscrire toute communication faite en vertu des paragraphes 6° à 10° du premier alinéa. Cette inscription fait partie du dossier. », ainsi que comme nous l'avons souligné à même l'article 18.2, ces renseignements communiqués pour des fins de recherches ne doivent pas être « structurés » de façon à permettre la corrélation de ceux-ci. Cela dit, ce dernier élément parait inapproprié avec l'essor des mégadonnées (big data)[468].

Considérant ce que nous avons exposé en ce qui a trait à la notion d'entreprise définie à l'article 1525 du C.c.Q. et étant donné que nous considérons certaines activités de recherche comme l'exploitation d'une entreprise, l'article 20 de la LPRPSP vient donc prendre assise :

> « Dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à tout préposé, mandataire ou agent de l'exploitant ou à toute partie à un contrat de service ou d'entreprise qui a qualité pour le connaître qu'à la condition que ce

---

[467] LPRPSP, art. 18.2.

[468] Comme nous l'avions souligné au second chapitre de la première section de ce mémoire, ces mégadonnées sont liées étroitement à la recherche. Bien que ce mémoire ne vise pas ces immenses banques de données informatique permettant de combiner et d'analyser l'informations, il n'en demeure pas moins qu'ils suscitent des questionnements notamment au droit à la vie privée puisque ces mégadonnées peuvent comprendre des renseignements personnels.

> renseignement soit nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat ou de son contrat. »[469].

À cet égard, les auteurs Lukasz Granosik et Kateri-Anne Grenier soutiennent que :

> « […] Lorsqu'un renseignement personnel est rendu accessible à l'extérieur de l'entreprise ou à un agent ou un mandataire, et ce, sans le consentement de la personne concernée, l'entreprise détentrice du renseignement doit faire en sorte que l'exécution du mandat ou de la délégation de fonction soit suffisamment encadrée, en tenant compte de la lettre et de l'esprit de la loi. Il est ainsi plus aisé de déterminer si les prescriptions de l'article 20 sont respectées ou non. Cette précaution est également nécessaire compte tenu de l'obligation faite à l'entreprise en vertu de l'article 10 de la loi. »[470].

Cette réflexion s'arrime également avec celle de Jean-François de Rico formulant que la Commission d'accès à l'information interprète la LPRPSP comme « *exigeant la conclusion d'un contrat écrit* »[471] en référence à la décision *Deschênes* c. *Groupe Jean Coutu (P.J.C.) inc.*[472]. Cette importante décision précise que les mandataires ont la possibilité d'avoir accès aux renseignements personnels lorsque le contrat précises dans son écrit les éléments suivants:

> « […]
>
> a) la portée du mandat;
> b) les buts pour lesquels le mandataire (ou l'agent) utiliserait les renseignements (l'objet du dossier);
> c) la catégorie de personnes qui aurait accès aux renseignements;
> d) l'obligation d'assurer la confidentialité des renseignements.
> »[473].

En effet, la Commission ajoute même que :

---

[469] LPRPSP, art. 20.
[470] Lukask GRANOSIK et Kateri-Anne GRENIER, *La Loi sur la protection des renseignements personnels dans le secteur privé : 2e édition annotée*, Cowansville, Édition Yvon Blais, 2013 p. 52.
[471] J-F DE RICO, préc., note 240.
[472] *Deschesnes* c. *Groupe Jean Coutu (PJC) inc.*, 13 juillet 2000, (C.A.I.) 13 juillet 2000, Commission d'accès à l'information du Québec EYB 2000-178499.
[473] Karl DELWAIDE, « Protection de l'information et de la vie privée », FASKEN, 2006, en ligne < https://www.fasken.com/fr/solution/practice/privacy-and-cybersecurity#sort=%40fclientworksortdate75392%20descending>, (consulté le 28 avril 2019).

> « Sans ces mesures de sécurité que constitue la signature de ces contrats, Dieu sait jusqu'où et jusques à quand l'information […] pourra circuler en dehors de tout contrôle […] »[474] (nos soulignements).

Dans la mesure où cette affirmation avait déjà de l'importance au tout début des années 2000, il nous apparaît évident, dans le contexte de ce mémoire, que le contrat est essentiel afin de lier toutes les parties impliquées. Logiquement, les proportions des fuites seront exponentielles lorsque l'information est portée sur un environnement en ligne.

En l'occurrence, que les activités de recherche s'effectuent sur une IaaS ou dans un cadre informatique plus conservateur, le contrat occupe déjà une place prédominante pour la recherche. En effet, des ententes sont contractées entre autres afin de définir la propriété intellectuelle visée et les personnes admissibles ainsi que pour préciser les modalités de partage des revenus et du transfert technologique advenant la commercialisation d'une invention. Ces ententes lient habituellement trois acteurs : les chercheurs, l'université et des partenaires industriels. Parfois, elles pourront être encadrées par des services de facilitateur[475] incluant, mais ne se limitant pas à : aligo[476], univalor[477] ou sovar[478] formant alors une relation multipartite[479]. À cet effet, la politique sur la propriété intellectuelle de l'Université de Montréal prévoit que :

> « Lorsqu'un organisme des secteurs publics, parapublic, privé ou communautaire, autre qu'un conseil subventionnaire ou une entité assimilable, contribue financièrement ou participe conjointement avec un chercheur de l'Université à la réalisation d'activités de recherche, de création, de développement ou d'enseignement, ces activités font l'objet, en règle générale, d'une entente écrite entre l'Université et l'organisme. »[480].

---

[474] *Deschesnes* c. *Groupe Jean Coutu (PJC) inc.*, 13 juillet 2000, (C.A.I.) 13 juillet 2000, Commission d'accès à l'information du Québec EYB 2000-178499.

[475] « Société de valorisation. », voir notamment Service Québec, en ligne : <http://www.fil-information.gouv.qc.ca/Pages/Article.aspx?idArticle=2608105624>, (consulté le 28 avril 2019).

[476] « Aligo Innovation » est une société de valorisation de la recherche universitaire Québecoise provenant du regroupement des sociétés Gestion Valeo et MSBi Valorisation. Aligo valorise les actifs de propriété intellectuelle de ses partenaires institutionnels, voir en ligne : <https://www.aligo.ca/>, (consulté le 28 avril 2019).

[477] Univalor, voir en ligne : <https://univalor.ca/>, (consulté le 28 avril 2019).

[478] Sovar, est une Société de valorisation de la recherche universitaire, voir en ligne : <https://www.sovar.com/>, (consulté le 28 avril 2019).

[479] Dans les développements d'innovation en technologies de la santé par exemple, la relation contractuelle pourrait lier le chercheur, l'université, le partenaire industriel, la société de valorisation, et même le Consortium industriel de recherche et d'innovation en technologies médicales MEDTEQ.

[480] *Id., préc.,* note 457.

En plus des acteurs visés actuellement par ces ententes, il sera nécessaire de lier les tiers pouvant avoir accès à l'infrastructure infonuagique. Puisque comme nous l'avons démontré[481], un prestataire de service infonuagique pourrait avoir à intervenir sur une infrastructure pour corriger ou se prémunir contre une vulnérabilité[482].

Plusieurs litiges furent entendus par les tribunaux sur des différends concernant des données de recherche protéger par droit d'auteur[483]. En revanche, nous constatons qu'aucun cas incluant un tiers offrant des services infonuagiques ne s'est rendu devant les tribunaux canadiens. Néanmoins, on constate à la lecture de la jurisprudence que :

> « […] l'utilisation de ressources ou services [d'une université] pour l'exécution de travaux de R-D donne des droits sur les résultats de ces travaux [à l'université] »[484].

D'ailleurs, il importe également de préciser que les « services informatiques » et « les réseaux de communications électroniques » sont considérés comme des ressources ou services. Ainsi qu'adviendrait-il du fait que les ressources utilisées pour la création du contenu protégé sont celle d'un tiers ? Il faudra donc que les ententes contractuelles, requises par les politiques et règlements universitaires prévoient des exclusions quant aux partages de la propriété intellectuelle avec les prestataires de service infonuagique.

### 2.1.2 Les données d'enseignements visées par les lois spécifiques au secteur privé

Comme il a été mentionné, outre les quelques points signalés au chapitre précédent, la possible impartition de ce type de données vers l'infonuagique ne semble pas poser des contraintes dans un contexte régi par les lois s'appliquant aux organisations publiques. Il en va de même pour les règles destinées aux entreprises privées. Les données nécessitantes une

---

[481] Voir les risques associés à l'utilisation d'IaaS au second chapitre de la première partie ainsi que leurs explications, voir Annexe 1 : Analyse de Risque.
[482] Voir Annexe 1 : Analyse de Risque, R13.
[483] Voir notamment *Fardad* c. *Corporation de l'École polytechnique de Montréal*, 2007 QCCS 5430;
*Corporation de l'École polytechnique de Montréal* c. *Fardad* 2010 QCCA 992;
*Beaudoin* c. *Université de Sherbrooke* 2007 QCCS 2291; et
*Plastiques Gagnon inc.* c. *Audace technologies inc.* 2006 QCCS 69;
[484] *Id*.

protection particulière issue des règles s'appliquant aux entreprises privées seront encore ici liées à des questions de confidentialité ainsi qu'a des notions de droit d'auteur. En effet, dans le cadre de certains cours offerts dans les universités, des ententes de confidentialité pourraient avoir été signées avec des partenaires industriels afin d'enseigner une technologie protégée par droit d'auteur ou par un brevet[485]. Que ce soit de simples données statistiques, des manuels de cours complexes ou des technologies scientifiques de pointes, tous ces documents sont protégés par la *Loi sur le droit d'auteur*[486]. Cette dernière s'appliquera ici également, rappelons que nous avons déjà cité sa fonction au chapitre précédent. Certes quelques exceptions sur le droit d'auteur s'appliquent aux établissements d'enseignement[487], mais certainement pas quand des indications à cet égard sont expressément mentionnées sur du matériel de cours. Nous devons d'ailleurs insister que selon plusieurs auteurs:

> *« Copyright laws are a major consideration for businesses considering cloud computing, as there are serious copyright and confidentiality concerns once you start putting your data in the cloud computing environment. »*[488].

Il est à noter que, avant d'enregistrer ou de traiter des œuvres protégées par le droit d'auteur sur une IaaS, il est nécessaire de vérifier les conditions d'utilisation de celui-ci[489]. En effet, il est indispensable de déterminer qui demeurera propriétaire des données entreposées et utilisées sur l'infrastructure infonuagique.

De plus, lorsqu'il est question d'activités pédagogiques, notamment de recherches, mais principalement d'enseignements il est en généralement plus aisé pour les universités d'obtenir des licences d'utilisations d'œuvres protégées par de la propriété intellectuelle. Selon l'Avis du Conseil de la science et de la technologie, « […] ce n'est pas le transfert technologique qui attire en premier lieu l'entreprise, mais l'accès à l'expertise en recherche (excellence) et aux

---

[485] Notons que les brevets en instance ne devraient aussi, ne pas être hébergé ou traité sur une IaaS.
[486] *Loi sur le droit d'auteur*, LRC 1985, c C-42.
[487] Voir notamment, les licence de reproduction Copibec - Société québécoise de gestion collective des droits de reproduction, en ligne : <https://www.copibec.ca/>, (consulté le 28 avril 2019).
[488] Anne S.Y. Cheung, Rolf H. Weber. George Yijun Tian, *Privacy and legal issues in cloud computing*, Cheltenham, Edward Elgar Publishing, 2016, p. 165.
[489] Christian SOLMECKE, «The Legal Aspect of cloud Computing under Copyright Law», *Wilde Beuger Solmecke*, (13 septembre 2013), en ligne : <https://www.wbs-law.de/eng/it-law/the-legal-aspects-of-cloud-computing-under-copyright-law-45886/>, (consulté le 28 avril 2019).

compétences des étudiants »[490]. Quoi qu'il en soit, des donations de licences permettant l'utilisation de logiciels scientifiques, la communication d'information confidentielle ou encore de technologies dans le cadre de cours est fréquente et leurs traitements ou leurs entreposages dans une IaaS devraient être permises par l'entente contractuelle conclue avec l'entreprise propriétaire des données.

### 2.1.3 Les données de gestion visées par les lois spécifiques au secteur privé

À première vue, nous pourrions avoir l'impression que le droit s'appliquant au secteur privé ne devrait pas avoir d'incidence sur les données de gestions des universités, mais il en est tout autrement. En dépit de la mention de Pierre-André Côté, soulevant que « les lois fiscales ont traditionnellement été interprétées de manière restrictive […] »[491] et donc ne peuvent pas être utilisées pour expliquer le fonctionnement des universités, il est tout de même intéressant de souligner que, dans le droit fiscal, les universités sont traitées comme des entreprises privées. En effet, pour tout ce qui a trait aux données de natures financières, comme le mentionne chaque rapport annuel de l'Université du Québec et des établissements du réseau :

> « […] tous les établissements du réseau de l'Université du Québec, répond à la définition d'un organisme sans but lucratif du secteur public et, en conséquence, devrait appliquer les Normes comptables canadiennes pour le secteur public […]. Les autres universités québécoises, hors du réseau de l'Université du Québec, répondent plutôt à la définition d'un organisme sans but lucratif du secteur privé et, en conséquence, devraient appliquer les Normes internationales d'information financière ou les Normes comptables Canadiennes pour les organismes sans but lucratif. Dans un souci d'uniformité, il a été convenu entre le MEES et les universités que toutes les universités québécoises préparent leurs états financiers en appliquant un référentiel comptable unique, soit les Normes comptables Canadiennes pour les organismes sans but lucratif. »[492] (nos soulignements).

---

[490] Ghislain ROUSSEL, « La gestion de la propriété intellectuelle dans les relations entre l'université et l'entreprise : pour une véritable dynamique d'alliances stratégiques; ; Propriété intellectuelle et université – entre la libre circulation des idées et la privatisation des savoirs ; Université inc. – des mythes sur la hausse des frais de scolarité et l'économie du savoir », Les cahiers de propriété intellectuelle, 2012, en ligne : < https://cpi.openum.ca/files/sites/66/Propriété-intellectuelle-et-université.pdf>, (consulté le 28 avril 2019).; Conseil de la science et de la technologie, « La gestion de la propriété intellectuelle dans les relations entre l'université et l'entreprise : pour une véritable dynamique d'alliances stratégiques », Ministère du Développement économique, de l'innovation et de l'Exportation, Gouvernement du Québec 2011, en ligne : < http://collections.banq.qc.ca/ark:/52327/bs2103875>, (consulté le 28 avril 2019).

[491] Pierre-André CÔTÉ, *Interprétation des lois*, 4e éd., Montréal, Les Éditions Thémis, 2009, p. 562.

[492] Ministère de l'Éducation et de l'Enseignement supérieur, « Rapport Annuels de l'Université du Québec et de ses établissements », en ligne : <https://www.uquebec.ca/reseau/fr/publications/rapports-annuels>, (Consulté le 28

Cependant, bien que les normes comptables attribuables aux OSBL privés s'appliquent à l'ensemble des universités québécoises, ces normes ne comportent aucune mention qui pourrait potentiellement proscrire la communication ou le traitement de l'information dans une IaaS[493].

Quant aux données de gestions relatives aux ressources informationnelles, comme pour bien d'autres types de données présentes dans les organisations, la réserve quant à leur utilisation ou leur traitement dans des systèmes infonuagiques ressort de la classification de ces données. Nous traiterons de cette question dans la section ci-après.

### 2.1.4 Les données concernant les étudiants et les membres du personnel visées par les lois spécifiques au secteur privé

Nous avons décidé de joindre les données concernant les étudiants et les membres du personnel des universités, puisque, selon la logique, ces derniers recevront le même traitement au point de vue de la LPRPSP.

Premièrement, nous savons que, tel que précisé par la commission d'accès à l'information du Québec, « Depuis le 1er janvier 1994, les associations étudiantes sont assujetties à la *Loi sur la protection des renseignements personnels dans le secteur privé.* »[494]. En ce qui concerne les syndicats, leurs statuts demeurent nébuleux[495]. Selon notre analyse, et par souci de cohérence, nous sommes d'avis qu'ils devraient avoir les mêmes devoirs envers la loi. En effet, il est important de préciser que dans *Girard* c. *Association des courtiers d'assurances du Québec*, le juge Desmarais de la Cour du Québec conclut que « [l]'échange de

avril 2019); Tous les rapports annuels de l'université du Québec et des établissements du réseau des dernières années comportent cette mention qui semble être reprise du Cahier des définitions, des termes et des directives de présentation du Système d'information financière des universités.

[493] Institut Canadien des Comptables Agréés, « Guide sur les normes comptables pour les organismes sans but lucratif canadiens », Canadien, 2012. en ligne : <https://www.cpacanada.ca/-/media/site/business-and-accounting-resources/docs/guides-normes-comptables-osbl-sept-2012_20021.pdf?la=fr&hash=2CFAB131F906C4B2B6DA9B4A34990416C735FD1A>, (consulté le 28 avril 2019).

[494] *Id*. préc., note 155.

[495] *Conseil de presse du Québec* c. *Lamoureux-Gaboury*, 2003 QCCQ 33002.

services au sein d'une communauté professionnelle constitue une activité économique organisée et donc qu'il remplit cette condition essentielle de l'entreprise. »[496].

En lien avec notre réflexion, la cour s'est penchée sur une cause où elle mentionne expressément que la société d'État québécoise Hydro-Québec, qui comporte elle aussi des syndicats et des associations au même ordre que les universités, tel que tout autre établissement d'enseignement est bel et bien régi par la LPRPSP[497]. La cour d'appel a également été invitée à se prononcer sur la question en devant établir le statut juridique d'une entité dans *Commission d'accès à l'information* c. *Conseil de presse du Québec*, mais elle a décliné[498]. Elle rappelle cependant « […] que la détermination de ce qui constitue une entreprise au sens de l'article 1 de la LPRPSP procède du cas par cas. […]»[499].

Quoi qu'il en soit, étant donné que les dossiers conservés dans les établissements seront composés inévitablement de renseignements personnels au sens de l'article 2 de la LPRPSP[500] et puisque la CAI, inspirée de l'article 10 de la LPRPSP, précise que les associations étudiantes ont « l'obligation de ne recueillir que les renseignements personnels nécessaires à l'objet du dossier et d'en assurer la confidentialité par des mesures de sécurité adéquates[501] » (nos soulignements), nous sommes d'avis qu'ils ont les mêmes obligations qu'une entreprise privée. Évidemment, sans nécessairement avoir l'expertise souhaitée pour assurer la confidentialité de ces dossiers.

Tel que nous l'avions mentionné au chapitre précédent, encore une fois, tout comme en ce qui a trait à l'article 70.1 de la *Loi sur l'accès*, une analyse approfondie des lois relatives à la protection des renseignements personnels s'appliquant à la juridiction où à l'organisme privé prodiguant les services d'IaaS doit être fait. Ces propos sont essentiels puisque l'article 17 de la LPRPSP prévoit « […] la possibilité de recourir aux services d'un prestataire dont les

---

[496] *Girard* c. *Association des courtiers d'assurances du Québec*, [1997] R.J.Q. 206.
[497] *J.D.* c. *Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 (SCFP)*, 2011 QCCAI 279.
[498] *Commission d'accès à l'information* c. *Conseil de presse du Québec*, 2006 QCCA 1282.
[499] *Id*.
[500] LPRPSP, art 2., « *Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.* ».
[501] *Id*. préc., note 155.

installations sont sises à l'extérieur du Québec aux fins de détention, d'utilisation ou de communication pour son compte […] »[502].

Cependant, rappelons que, tel qu'il est indiqué dans l'« Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », 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. »[503].

Nous sommes donc d'avis que les syndicats et les associations des établissements d'enseignement doivent user de prudence avant de recourir à l'utilisation d'une IaaS publique pour certaines données personnelles, mais que la loi ne l'interdira pas explicitement. Néanmoins, rappelons que notre analyse dénote des normes plus restrictives imposées aux organismes publics qu'aux entreprises privées.

## 2.2 La classification des données visées par les lois s'appliquant au secteur privé

Tout comme nous l'avons mentionné en ce qui concerne les règles obligataires spécifiques aux organismes publics, la classification de l'information est foncièrement liée à l'importance des données téléversées ou traitée dans une IaaS. Étant donné que les organisations sont responsables de la protection des données qu'elles transfèrent au fournisseur d'IaaS[504], elles doivent voir à ce que les données de classification les plus névralgiques soient traitées de manière appropriée. Ainsi, comme ce fût le cas pour leur homonyme public, certaines des lois attribuables aux domaines privés s'immisceront également aux différents types d'information présents dans les universités.

---

[502] J-F DE RICO, préc., note 240, p. 4.
[503] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 45.
[504] *Id*., préc., note 358.

### 2.2.1 Les données publiques visées par les lois s'appliquant au secteur privé

Dans la mesure où les données ciblant ce groupe ont une étiquette publique, il ne devrait pas y avoir de contrainte à être traité sur une IaaS. En effet, comme il est prévu au premier article de la LPRPSP, « […] la présente loi ne s'applique pas à un renseignement personnel qui a un caractère public en vertu de la Loi. »[505]. De plus, même si nous réfléchirons davantage sur la LPRPDÉ, lorsque nous aborderons l'élément de la disponibilité issue de la triade DIC, nous devons tout de même mentionner d'emblée que, malgré le risque de communication transfrontalier des renseignements des employés ou des chercheurs universitaires, la LPRPDÉ dispose que les « coordonnées d'affaires » d'un individu ne sont pas des renseignements personnels au sens de la loi.

Les coordonnées d'affaires sont définies comme :

> « Tout renseignement permettant d'entrer en contact — ou de faciliter la prise de contact — avec un individu dans le cadre de son emploi, de son entreprise ou de sa profession, tel que son nom, son poste ou son titre, l'adresse ou les numéros de téléphone ou de télécopieur de son lieu de travail ou son adresse électronique au travail. »[506].

Elles pourront, quant à elles, être aussi traitées à même une IaaS. Outre les coordonnées d'affaires, l'information dite publique est tout à fait propice à être traitée dans les nuages, peu importe leurs localisations ou leurs degrés de conformité aux risques.

### 2.2.2 Les données internes/privées visées par les lois s'appliquant au secteur privé

En ce qui a trait aux données internes et privées, nous l'avons déjà mentionné dans notre définition préalable, elles sont composées de toutes les données institutionnelles qui ne sont pas expressément classées sous les rubriques des données confidentielles, restreintes ou publiques. Nous avons entre autres soulevé certaines informations rattachées à des licences institutionnelles ou de recherches. Ces informations pourraient être liées, tout comme certaines données d'enseignements ou de recherche, à des clauses de non-divulgation ou de restriction

[505] LPRPSP, art. 1, al. 1.
[506] *Id*., art. 2, al. 1.

d'utilisation.[507] Comme nous le verrons en fond dans la section traitant de la triade, ces données sont ciblées par des lois s'appliquant au secteur privé, entre autres, mais surtout lorsqu'ils voyageront sur les réseaux informatiques. En effet, il est monnaie courante qu'une université partage des licences informatiques via l'accès à un réseau privé virtuel sécurisé, ou VPN[508] à ces utilisateurs et l'utilisation de logiciels institutionnels sur une IaaS ne fera que l'accentuer. L'effet de ce type d'utilisation et du transfert sur les réseaux de télécommunication de ces ressources, dont les propriétaires sont des entreprises privées, est protégé par la LPRPDÉ. Outre ces quelques exceptions, l'emploi d'une IaaS pour cette classification de données ne semble aller à l'encontre d'aucune obligation législative identifiée.

### 2.2.3 Les données confidentielles et les données à accès restreint visées par les lois s'appliquant au secteur privé

Il nous apparaît juste d'articuler que dans un contexte universitaire comme dans bien des milieux, l'information confidentielle et les données à accès restreint seront de la plus haute importance. Naturellement, si ces données sont traitées dans une IaaS, elles pourront être circonscrites par des lois s'appliquant au domaine privé. Notamment par des articles de la LCCJTI qui ciblent, entre autres, le caractère confidentiel des données en y faisant référence plus d'une dizaine de fois. Nous reviendrons sur ce point dans la section subséquente traitant spécifiquement de l'obligation de confidentialité dans un contexte de droit spécifique au secteur privé. Dans un deuxième temps, la LPRPSP sera aussi interpelée, selon certaines circonstances particulières attribuables aux types de données. Par exemple, lorsque des renseignements personnels sur des employés d'une université sont détenus par un syndicat tel que vu précédemment[509] ainsi que pour toute propriété intellectuelle lié à des données de recherches.

---

[507] Notamment des restrictions relatives à l'endroit où le logiciel est utilisé. C'est le cas notamment des logiciels de la compagnie Ansys qui limite l'usage à 40KM du site désigné au contrat. En conséquence, ces logiciels ne pourront vraisemblablement pas être utilisés sur une IaaS. « "*LAN License" means a license of the Program(s) that permits Licensee's and its Affiliates' employees and Contract Users located within a 25-mile (40-km) radius of the Designated Site to use the Program(s).*»; voir ANSYS « Software License Agreement », 28 décembre 2018, en ligne : < https://www.ansys.com/-/media/ansys/corporate/files/pdf/footer/wla-december-28-2018.pdf?la=en>.

[508] OQLF., préc., note 10, « VPN/RPV » : *« Réseau étendu privé établi en créant des liaisons permanentes spécialisées entre réseaux internes à travers des réseaux publics afin de répondre aux besoins en partage des ressources des utilisateurs. ».*

[509] *Commission d'accès à l'information* c. *Conseil de presse du Québec*, 2006 QCCA 1282.

Sur le plan de la sémantique, force est de constater que, dans le milieu universitaire, ce ne sera pas tant la classification des données qui influencera la possibilité d'impartition vers des systèmes infonuagiques, mais bien les types de données liés à des activités impliquant le secteur privé au sein des universités.

## 2.3 L'obligation de sécurité découlant des lois spécifiques au secteur privé

Afin de déterminer les obligations de sécurité imputables au droit s'appliquant au domaine privé dans les universités, nous devons à nouveau faire un travail introspectif sur la triade CID. Certes, comme nous l'avons vu jusqu'ici, certaines notions du droit s'appliquant au domaine privé peuvent avoir des incidences sur le choix de procéder à une externalisation des ressources informatiques dans les établissements universitaires. Il advient que malgré ces obligations, dans le cas d'une relation tripartite entre l'université, un bailleur de fonds privé et un hébergeur, ce dernier sera lui aussi soumis aux conditions des lois ciblant les entreprises privées. Si le choix est d'opérer une infrastructure à l'extérieur du Québec, comme nous l'avons vu, la communication des données « indépendamment du degré de sensibilité des renseignements visés »[510] nécessitera la conclusion d'une entente contractuelle, comme le prévoit entre autres l'article 17 de la LPRPSP précédemment cité, en plus de se conformer aux obligations qui suivront et qui forment notre triade.

### 2.3.1 L'obligation d'assurer la confidentialité des données

D'entrée de jeux, nous croyons que les entreprises prennent très au sérieux les questions liées à la confidentialité des données en général, non seulement quant aux renseignements personnels ou confidentiels. En effet, comme nous avons pu le constater au cours de nos recherches, les compagnies sont enclines à vouloir protéger les données présentes sur les systèmes infonuagiques ou, du moins, c'est ce qu'elles indiquent aux utilisateurs. Il suffit de poser le regard sur l'affaire *United States* c. *Microsoft*[511] survenue récemment. Ce jugement

[510] J-F DE RICO, préc., note 240, p. 7.
[511] *Microsoft* v. *United States*, No. 14-2985 (2d Cir. 2016); *Microsoft Corp.* v. *United States*, No. 14-2985 (2d Cir. 2017).

expose la portée et l'importance qu'accordent les fournisseurs de services à la confidentialité de nos données personnelles. Dans ce cas, Microsoft s'est battue devant la plus haute instance américaine afin de faire valoir la confidentialité des données des entreprises et des utilisateurs de ses services infonuagiques. En résumé, les données visées par un mandat étaient stockées par Microsoft sur des serveurs situés en Irlande. Microsoft contesta alors le mandat de perquisition et refusa de communiquer les éléments demandés au motif que la loi américaine ne peut avoir une portée extraterritoriale. En première instance, la légitimité du mandat fut confirmée par le juge[512]. Toutefois, l'*« United States Court of Appeals – for the second circuit »* est venue confirmer les arguments de Microsoft et le mandat fut annulé[513]. En vain, cette décision velléitaire ne suffit pas à fixer la jurisprudence sur cette question puisque d'autres cas suivirent proposant un dénouement opposé[514], proposant que la seule considération découle du lieu géographique d'édification du fournisseur infonuagique et non de l'emplacement physique des serveurs. Pour décider si la présomption d'extraterritorialité limite la portée d'une disposition législative, les tribunaux américains appliquent un critère en deux parties[515]. Premièrement, « il s'agit de déterminer si la loi donne une indication claire et affirmative qu'elle a une portée extraterritoriale. »[516] (notre traduction). Dans la négative, la cour doit alors déterminer « si l'affaire concerne une application nationale de la Loi. »[517] (notre traduction). Parmi les cas contradictoires, mentionnons celui de Google[518], dans lequel il a été déterminé que le « Stored Communication Act »[519] n'avait pas de portée extraterritoriale, mais que le deuxième critère s'appliquait puisque la faute reprochée se déroulait aux États-Unis. Ainsi, Google dut exécuter le mandat de perquisition.

---

[512] *In the matter of Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp*., Case No. 15 F. Supp. 3d (S.D.N.Y. 2014).
[513] *Id*. Préc., note 511.
[514] Voir notamment : *In the matter of Two email accounts stored at Google, Inc.*, Case No. 17-M-1234, 17-M-1235 2017 WL 706307 (e.D. Wis. Feb. 21, 2017); ainsi que *In The Matter Of The Search Of Content Stored At Premises Controlled By Google Inc.* Case No. 16-mc-80263-RS.
[515] *Morrison* v. *National Australia Bank Ltd*., 561 U.S. 247, 261-70 (2010).
[516] In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, No. 3:2016mc80263 - Document 45 (N.D. Cal. 2017).
[517] *Id*.
[518] *Id*.
[519] *Stored Communications Act* (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712).

Voyant l'opposition sur la question, le cas de Microsoft fut porté vers la Cour Suprême. Toujours est-il qu'aucune décision ne fût rendue puisque le « *Clarifying Lawful Overseas Use of Data Act* » connut sous le nom du « *CLOUD Act* » est venue trancher la question du litige[520]. Le Cloud Act amende le Store Communications Act, 18 U. S. C. § 2701 et suiv., en ajoutant la disposition suivante:

> « *A* [service provider] *shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.*»[521].

Ainsi, tel qu'il est précisé par la Cour suprême des États-Unis :

> « *... No live dispute remains between the parties over the issue with respect to which certiorari was granted.* […] *Further, the parties agree that the new warrant has replaced the original warrant. This case, therefore, has become moot. Following the Court's established practice in such cases, the judgment on review is accordingly vacated, and the case is remanded to the United States Court of Appeals for the Second Circuit with instructions first to vacate the District Court's contempt finding and its denial of Microsoft's motion to quash, then to direct the District Court to dismiss the case as moot.* »[522] (nos soulignements).

Tel que le précise Patrick J. Gallagher :

> « *While it may appear that Congress has effectively decided the case in the government's favor, Microsoft—and other technology companies—have welcomed the CLOUD Act because it provides more consistency than the outdated legislation did.* »[523].

---

[520] *United States* v. *Microsoft Corp*., 584 U. S. ___ (2018) (per curiam); Laurence HURLEY, «U.S. top court rules that Microsoft email privacy dispute is moot.» *Reuters*, 17 Avril 2018, en ligne : «https://www.reuters.com/article/us-usa-court-microsoft/supreme-court-rules-that-microsoft-email-privacy-dispute-is-moot-idUSKBN1HO23S». (consulté le 28 avril 2019).

[521] *Id.*

[522] *United States* v. *Microsoft Corp*., 584 U. S. ___ (2018) (per curiam).

[523] Patrick J. GALLAGHER, «The CLOUD Act: Mooting the Microsoft Ireland Case, but not forecasting clear skies just yet. », *Columbia Business Law Review, 13 Avril 2018,* en ligne : <https://cblr.columbia.edu/the-cloud-act-mooting-the-microsoft-ireland-case-but-not-forecasting-clear-skies-just-yet/>, (consulté le 28 avril 2019).

De plus, il est intéressant de noter que les trois grands fournisseurs démontrent une très grande transparence des demandes d'informations imposées par la loi. En effet, toutes ces informations sont facilement accessibles en ligne[524], ce qui permet d'ailleurs de constater que Microsoft a transmis des données[525] provenant de l'Irlande pendant la période visée par le nouveau mandat en lien avec ce litige.

Afin de réitérer leur position, Microsoft a émis 6 principes[526] entourant la confidentialité de l'information entreposés sur des systèmes infonuagiques, les voici :

1. ***The universal right to notice*** *– Absent narrow circumstances, users have a right to know when the government accesses their data, and cloud providers must have a right to tell them.*
2. ***Prior independent judicial authorization and required minimum showing*** *– Law enforcement demands for content and other sensitive user data must be reviewed and approved by an independent judicial authority prior to enforcement of the order, and only after a meaningful minimum legal and factual showing.*
3. ***Specific and complete legal process and clear grounds to challenge*** *– Cloud providers must receive detailed legal process from law enforcement to allow for thorough review of the demand for user data, and must also have clear mechanisms to challenge unlawful and inappropriate demands for user data.*
4. ***Mechanisms to resolve and raise conflicts with third-country laws*** *– International agreements must avoid conflicts of law with third countries and include mechanisms to resolve conflicts in case they do arise.*
5. ***Modernizing rules for seeking enterprise data*** *– Enterprises have a right to control their data and should receive law enforcement requests directly.*
6. ***Transparency*** *– The public has a right to know how and when governments seek access to digital evidence, and about the protections that apply to their data.*

---

[524] Voir notamment : Microsoft Law enforcement requests, en ligne : <https://www.microsoft.com/en-us/corporate-responsibility/lerr>; Google Transparency report, en ligne : <https://transparencyreport.google.com/user-data/overview>; Amazon Information Request Reports, en ligne : <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF>; (consulté en avril 2019).

[525] Ici, les données ayant été communiqué sont définies comme étant : « Content is what our customers create, communicate, and store on or through our services, such as the words in an email exchanged between friends or business colleagues or the photographs and documents stored on OneDrive or other cloud offerings such as Office 365 and Azure. ».

[526] Microsoft Corporation, «Six Principles For International Agreements Governing Law- Enforcement Access To Data», en ligne : <https://blogs.microsoft.com/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf>, (consulté le 28 avril 2019).

Ces énoncés ainsi que leurs explications respectives[527] font connaître clairement l'importance que Microsoft prodigue à la confidentialité de l'information. Le président et directeur juridique de Microsoft, Brad Smith, mentionna que :

> *«…The following principles will guide our advocacy as governments shape international legal frameworks that address these critical questions. These principles also build on our ongoing efforts to protect our customers' data and enhance their privacy.* »[528].

Notons que Microsoft n'est pas la seule compagnie à avoir adopté des principes afin de répondre aux questions de traitement transfrontalier des données. Dans la foulée du CLOUD Act, Google a produit un cadre juridique[529] pour régir les demandes qu'ils reçoivent. Finalement, mentionnons qu'Amazon, a aussi publié un « *Data Residency Whitepaper* »[530] expliquant les fondements du Cloud Act ainsi que les rôles et responsabilités des acteurs impliqués dans leurs services infonuagiques.

Ces principes rappellent, entre autres le concept de « contrôle » des données. Rappelons que nous vivons dans une ère où les individus sont constamment invités à consentir à diverses activités de traitement des données sans nécessairement comprendre les risques encourus[531]. Le 5e principe de Microsoft évoque bien à cet effet que les entreprises, ou les organisations d'enseignements dans le cas qui nous concerne doivent conserver le contrôle de l'information porté sur les systèmes infonuagiques. C'est d'ailleurs, ce qui est visé par la LPRPSP au Québec.

Aussi, le premier principe invoqué par Microsoft vient sans difficulté rappeler les positions prises par le commissariat à la protection de la vie privée du Canada dans les nouvelles

---

[527] *Id.*, préc., note 526.
[528] Brad SMITH, « A call for principle-based international agreements to govern law enforcement access to data », Microsoft On the Issues, blog, 11 Septembre 2018, en ligne : <https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/>, (consulté le 28 avril 2019).
[529] Google, « Digital Security & Due Process: Modernizing Cross Border Government Access Standards for the Cloud Era » en ligne : <https://blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf>, (consulté le 28 avril 2019).
[530] Amazon Web Services, « Localisation des données Perspectives de la stratégie AWS », Juillet 2018, en ligne : <https://d1.awsstatic.com/whitepapers/compliance/FR_Whitepapers/Data_Residency_Whitepaper.pdf>, (consulté le 28 avril 2019).
[531] É. GRATTON., préc., note 160, p. 57.

obligations en matière de déclaration des atteintes aux données[532]. En effet, cette nouvelle obligation issue de la *Loi sur la protection des renseignements personnels numériques* vient exiger la déclaration des atteintes à la protection des données qui pourrait présenter un « risque réel de préjudice grave ». Cette déclaration obligatoire des atteintes aux mesures de sécurité prévoit une obligation à informer les propriétaires des données ou le gouvernement canadien lorsque des renseignements personnels sont visés par l'atteinte. Hélas, la loi américaine l'interdit. Ainsi, les prescriptions de l'article 8 de la LPRPSP ne pourront donc pas être respectées :

> « 8. La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer […] »[533].

Notons ici que les alinéas 2 et 3 de l'article 18 de la LPRPSP déjà cités prévoient d'emblée la possibilité à communiquer des renseignements récoltés « au directeur des poursuites criminelles et pénales […] » ainsi qu'« à un organisme chargé en vertu de la loi de prévenir, détecter ou réprimer le crime ou les infractions aux lois […] » qui auront en tout point de vue le même effet que le « *Cloud Act* » sur des données conservées sur des serveurs appartenant à un fournisseur de service infonuagique américain. Notons toutefois qu'il n'y a pas de logique à ce que le gouvernement américain recueille des données nous concernant.

En outre, le contrôle et la surveillance soutenus par le USA PATRIOT Act[534] n'est plus. L'article 215, en particulier, qui permettait au gouvernement la collecte massive de métadonnées a subi sa non-reconduction avec le « Sunset Clause » de cette loi[535]. Effectivement, en vertu du USA Freedom Act[536] maintenant en vigueur, les organismes gouvernementaux des États-Unis doivent désormais démontrer qu'il existe un motif raisonnable de croire que les informations

---

[532] *Règlement sur les atteintes aux mesures de sécurité*, DORS/2018-64.
[533] LPRPSP, art. 8.
[534] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, PUBLIC LAW 107–56—OCT. 26, 2001.
[535] Kate KNIBBS, « The US House Just Voted to Stop NSA's Bulk Data Collection*», Gizmodo,* 13 mai 2015, en ligne : <https://gizmodo.com/house-committee-votes-to-reform-usa-patriot-act-with-us-1700758645>, (consulté le 28 avril 2019).
[536] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, PUBLIC LAW 114-23 JUNE 2, 2015.

recueillies sont pertinentes à une enquête[537]. Ainsi en plus de nécessiter un agrément juridique, les organismes de sécurité et les agences de renseignements seront tenus de demander l'accès aux fournisseurs de services ayant la garde des données[538].

Aussi, tel que le mentionne l'auteur Jean-François De Rico, « des pouvoirs similaires sont accordés aux juges de la Cour fédérale du Canada sur demande du Service canadien du renseignement de sécurité. »[539]. Nous pouvons également ajouter à ceci la décision de l'arbitre dans « *The Board of Governors of Lakehead University and Lakehead University Faculty Association* » qui aborde la même position en affirmant :

> « *Indeed, […], privacy rights insofar as they exist in law are never absolute. Canadian courts may and do endorse subpoenas which probe into confidential information held by, for instance, banks and similar institutions. It would be surprising if the University could even begin to insulate its faculty from such intrusion. »*[540].

Rappelons aussi que cette pratique est loin d'être à terme, puisque comme l'indique l'auteur Karim Benyekhlef :

> « […] la sécurité [a constitué] une industrie pour l'État qui y a eu recours régulièrement afin d'affermir sa souveraineté et y trouver un brillant prétexte pour établir une surveillance et un contrôle toujours croissant sur ses citoyens, leurs activités et leurs affaires. »[541].

Il est donc clairement établi que le pouvoir intrusif que l'on reproche souvent à nos voisins du sud n'est pas limité à leur corpus législatif, il en est de même de la part des prescriptions canadiennes. Cela dit, les gouvernements canadien et étatsunien « partagent une relation en matière de défense qui est vaste »[542]. Ce lien permet, entre autres, l'échange de données avec

---

[537] Hogan LOVELLS, « Restoring Trust ? », International Association of Privacy Professionnal, 25 Juin 2015, en ligne : <https://iapp.org/news/a/usa-freedom-act-a-step-toward-restoring-trust/>, (consulté le 28 avril 2019).
[538] *Id*.
[539] J-F DE RICO, préc., note 240, p. 17.
[540] *Lakehead University (Board of Governors)* v. *Lakehead University Faculty Association*, 2009 ONLA 24632.
[541] Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation*, Montréal, Thémis, 2008, p. 685.
[542] Défense Nationale et Forces armées canadiennes, en ligne : <http://www.forces.gc.ca/fr/nouvelles/article.page?doc=relation-de-defense-entre-le-canada-et-les-etats-unis/hob7hd8s>, (consulté le 28 avril 2019).

nos autorités voisines[543] qui pourrait contrevenir aux lois s'appliquant au secteur privé, comme démontré à ce chapitre.

Évidemment, nous sommes conscients que les seuls fournisseurs infonuagiques ne sont pas américains. Néanmoins, comme les prestataires de service infonuagique qui offre des IaaS en sol québécois sont, soit d'ici, ou des États-Unis, nous avons fait le choix de se concentrer sur le droit américain.

Bref, l'hébergement à l'étranger pourrait être envisagé, ou du moins il ne pourrait pas être refusé sous ces motifs. Il serait cependant plus convaincant si le pays dispose de règlementation équivalente à la LPRPSP ou encore à la *Loi sur l'accès*.

Tel que mentionné précédemment et comme le soulignent les auteurs de l'« Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement québécois » : « …Le fait de procéder au chiffrement des données avant de les déposer dans le nuage pourrait être une solution à envisager[…] »[544] (ce passage ciblait les données hébergées aux États-Unis). Néanmoins, la problématique reste là même si les données sont conservées en sol canadien, puisque les grands fournisseurs de service IaaS sont contrôlés par des personnes morales étatsuniennes, donc soumises au Cloud Act. Cependant, le fait est que, malgré qu'il soit possible de procéder au chiffrement des données statiques ainsi qu'en transit, il est utopique actuellement de penser effectuer toute forme de traitement de données sous cette technologie. Ainsi les critères prévus aux articles 25 et 26 de la LCCJTI préalablement cités, ne pourront être facilement respectées.

La problématique s'accentue dans le cas où l'un ou des risques exposés dans ce mémoire surviendraient lors d'une impartition vers une IaaS dans la circonstance où des documents en lien avec une entreprise privée sont traités. Prenons l'exemple d'une chaire de recherche industrielle. Dans l'éventualité où l'erreur humaine[545] d'un administrateur ou d'un utilisateur rendrait déverrouillées et exposées des données liées à ce projet, les risques de perte de contrôle sur l'information sera exponentiel comparativement à si ces informations avaient été sur une

[543] J-F DE RICO, préc., note 240, p. 10.
[544] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 131.
[545] Voir Annexe 1 : Analyse de Risque, R.23 Erreur humaine (interne ou externe).

infrastructure traditionnelle. Bien entendu, les données ainsi exhibées ne seront pas limitées au réseau universitaire, mais bien, possiblement à la planète tout entière[546]. De plus, si, par les activités de la chaire, des informations confidentielles sont traitées ou développées, la propriété intellectuelle qui en découle est, comme nous l'avons vu, soumise à des traités, des conventions et des contrats, pour lesquels les obligations pourraient faire l'objet de transgressions. Il importe d'ailleurs de souligner que l'université demeurera responsable des atteintes à la confidentialité des données lors des transferts transfrontaliers, car c'est à elle de veiller au respect des règles établies pour les services qu'elle contracte tel que mentionné dans la LPRPDÉ :

> « Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. » [547].

Les auteurs Lukasz Granosik et Kateri-Anne Grenier reprennent l'obligation de confidentialité prévue à l'article 10 de la LPRPSP[548], qui véhicule sensiblement le même esprit que le deuxième alinéa de l'article 26 de la LCCJTI, ils affirment que :

> « […] un commerçant contrevient à l'article 10 de la loi lorsqu'il conserve les renseignements personnels et confidentiels d'un client dans un classeur non verrouillé situé dans une pièce non verrouillée, ou d'une manière le rendant facilement accessible à tous […] »[549].

Le classeur de cette illustration pourrait facilement être l'espace de dépôt de données situé dans une infrastructure infonuagique tel que nous venons de le présenter[550]. Évidemment,

---

[546] Eric LE BOURLOUT, «Dropbox victime d'une faille de sécurité béante », *01net*, 21 juin 2011, en ligne : <http://www.01net.com/editorial/534667/dropbox-victime-d-une-faille-de-securite-beante/>, (consulté le 28 avril 2019).
[547] LPRPDÉ, principe 4.1.3.
[548] L. GRANOSIK et K-A. GRENIER, préc., note 470.
[549] *Stacey* c. *Sauvé Plymouth Chrysler* (1991) inc., [2002] R.J.Q. 1779, J.E. 2002-1147, REJB 2002-32362 (C.Q.).
[550] Rejoins l'essence de L'article 4.7.3 de l'annexe 1 de la LPRPDÉ qui prévoit que :
« Les méthodes de protection devraient comprendre :
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. ».

comme le rappelle David P. Whelan *« Once that information is stored on a computer, the potential for a more damaging revelation is increased. »*[551].

Considérant la relation tripartite impliquée dans l'impartition vers une IaaS, nous considérons que les requis de la loi évoquent des prérogatives obligataires trop imposantes pour accepter d'emblée une impartition vers des services infonuagiques. Nous croyons aussi que chaque cas, notamment lors d'ententes de développement avec des partenaires d'affaires privés pour de la recherche scientifique, devra être minutieusement analysé afin de s'assurer de respecter les clauses pouvant figurer aux contrats convenus entre les parties.

### 2.3.2 L'obligation d'assurer l'intégrité des données

L'intégrité est un élément clé de l'obligation de sécurité tout autant applicable aux organismes publics que pour ce qui est du secteur privé. D'ailleurs, il est important de rappeler que la LCCJTI s'appliquera intégralement à ces deux sphères d'activités. Comme l'obligation d'intégrité ne diffèrera pas pour ce qui est de ces deux secteurs, il est inutile de reprendre l'entièreté des articles traitant ce point.

Dans le chapitre précédent, nous avons soulevé promptement le cas *Digital Shape Technologies Inc.* c. *Comte*[552]. Nous allons maintenant approfondir l'étude de ce cas qui expose le caractère déontique de l'obligation d'intégrité lié à un environnement infonuagique.

Rappelons l'essence de ce cas, Digital Shape Technologies Inc. « […] a des motifs raisonnables de croire que les défendeurs ont dissimulés, altérés et détruits de la preuve pertinente au litige »[553]. Puisque cette preuve se trouve potentiellement sur des systèmes infonuagiques, le juge Stéphane Sansfaçon :

> « **O. ORDONNER** aux défendeurs Sébastien Comte, Anne Brisebois et Guillaume Joubert de divulguer à la firme d'experts KPMG le nombre et la nature des comptes de messagerie électronique dont ils sont présentement titulaires ou ont été titulaires, personnellement ou par le biais d'une société qu'ils contrôlent, incluant, mais sans limiter la généralité de ce qui précède,

[551] D. P. WHELAN, préc., note 259 p. 83.
[552] *Digital Shape Technologies Inc.* c. *Comte*, 2018 QCCS 1199.
[553] *Id.*

> Gmail, Yahoo, Hotmail, MySunrise et Outlook, dans les cinq (5) jours du jugement à intervenir;
>
> **P. ORDONNER** aux défendeurs Sébastien Comte, Anne Brisebois et Guillaume Joubert de divulguer à la firme d'experts KPMG le nombre et la nature des comptes infonuagiques dont ils sont présentement titulaires ou ont été titulaires, personnellement ou par le biais d'une société qu'ils contrôlent, incluant, mais sans limiter la généralité de ce qui précède, Google Drive, Dropbox et OneDrive, dans les cinq (5) jours du jugement à intervenir;
>
> **Q. ORDONNER** aux défendeurs Sébastien Comte, Anne Brisebois et Guillaume Joubert de donner accès à tous leurs comptes de messagerie électronique et comptes infonuagiques à la firme d'experts KPMG en leur procurant leurs noms d'utilisateur et mots de passe à jour; »[554].

Notons que certaines de ces demandes sont calquées sur le jugement du juge Stephen W. Hamilton, j.c.s. dans *Mag Energy Solutions inc.* c. *Falconer Cloutier*[555] donc ne serait pas abusive pour la préservation d'éléments de preuve. Rappelons que :

> « Pour conclure à un abus de procédure, le Tribunal doit être convaincu que la procédure est manifestement mal fondée, vouée à l'échec et que la partie qui l'a intenté était de mauvaise foi, a notamment fait preuve d'un comportement blâmable »[556]

Cependant, dans le cadre de son action contre ses ex-employés et malgré les impositions issues de la première instance, « Digital Shape Technologies inc. fait une demande de préservation et divulgation de la preuve, demande que les défendeurs veulent [néanmoins] faire déclarer abusive. »[557].

Les défendeurs « soutiennent que DST tente de trouver des éléments de preuve qui n'existent vraisemblablement pas et que sa demande va à l'encontre des règles de proportionnalité prévues au Code de procédure civile et de leur droit à la vie privée. » (nos soulignements)[558].

---

[554] *Id*.
[555] *Mag Energy Solutions inc*. c. *Falconer Cloutier*, 2016 QCCS 2830.
[556] *Digital Shape Technologies Inc.* c. *Comte*, 2018 QCCS 1199; Dans le cas présent, « On reproche à Mme Brisebois [l'un des défendeurs] d'avoir détruit certains courriels ». Rappelons qu'il en reviendra au juge du fond de trancher cette question, préc., note 439.
[557] *Digital Shape Technologies Inc.* c. *Comte*, 2018 QCCS 1199.
[558] *Id.*

Tout compte fait, toutes ces questions découlent du fait que l'intégrité de la preuve ne peut être prouvée facilement. L'intégrité est difficile à valider étant donné que les données recherchées sont entreposées sur des systèmes infonuagiques inaccessibles pour la partie Demanderesse.

Comme nous l'avons vu, il est pourtant relativement aisé de déterminer si une donnée informatique est intègre advenant l'accès à des journaux. Ce qui n'est pas le cas ici, puisque ces données étaient entreposées chez un fournisseur de service. Notons néanmoins que, selon la désambiguïsation de l'infonuagique présentée dans la toute première partie de ce mémoire, les services de courriel informatiques sont considérés comme des SaaS. Ces services logiciels, s'ils ne font pas partie intégrante d'une offre IaaS, n'auront pas de journaux intégrés permettant d'assurer un suivi sur l'intégrité des données, en contrepartie, la composition des informations y étant entreposée est habituellement inchangeable.

Bref, l'intégrité des fichiers que requiert cette cause n'est pas apodictique puisqu'elle n'est pas intégrée à une IaaS, mais plutôt conservée sur des comptes personnels appartenant aux employés. Le dénouement de procès en instance sera intéressant à suivre, du moment où il apparait évident à notre point de vue que les requis de l'article 17 de la LCCJTI n'ont pas été suivis. Ils prévoient que :

> « **17.** L'information d'un document qui doit être conservé pour constituer une preuve, qu'il s'agisse d'un original ou d'une copie, peut faire l'objet d'un transfert vers un support faisant appel à une technologie différente.
>
> Toutefois, sous réserve de l'article 20, pour que le document source puisse être détruit et remplacé par le document qui résulte du transfert tout en conservant sa valeur juridique, le transfert doit être documenté de sorte qu'il puisse être démontré, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée.
> […] »[559] (nos soulignements).

Or, comme l'expert dans cette cause, Paul Laurier, le mentionne dans une déclaration assermentée « […] je constate un changement de couleur (…) qui peut suggérer que ce courriel a été soit déplacé, soit copié, puis collé; »[560].

---

[559] LCCJTI, art. 17.
[560] *Digital Shape Technologies Inc*. c. *Comte*, 2018 QCCS 1199.

En résumé, quoique cette cause n'ait pas de lien intrinsèque avec les universités, nous considérons qu'elle permet de bien comprendre les subtilités encadrant l'obligation d'intégrité pouvant surgir d'une utilisation des IaaS ou du moins de l'infonuagique. De plus, elle évoque clairement, afin d'apprécier l'intégrité d'une donnée, la nécessité de la présence et de l'exactitude des journaux[561].

Comme pour le domaine public, la notion d'intégrité doit aussi être assurée tout au long du « *cycle de vie* » du document[562]. Rappelons que l'article 6 de la LCCJTI évoque également l'aspect de la destruction du document lorsqu'il a atteint sa fin de vie utile. Cet aspect sera accentué par l'utilisation de données liées à des entreprises ou à des activités en lien avec le domaine privé, puisque l'information liée à la recherche ne doit pas être conservée au-delà de la terminaison du contrat. Pour se faire, le contrat d'impartition vers une IaaS devra convenir des clauses à cet effet[563].

Un exemple de la nécessité de la suppression des données lors de la terminaison du contrat est mentionné par les auteurs de l'ouvrage « *Privacy and Legal Issues in Cloud Computing* », Il est inscrit concernant la recherche scientifique (sur le thème du génome humain) :

> « *They* [researchers] *should also ensure that they can retrieve genomic data when needed and that a CSP cannot retain it or use it after the contract ends, subject to legal or regulatory requirements and or authorization of the researchers. »*[564].

Bien entendu, nous croyons que cet énoncé peut aisément s'étendre à plusieurs, sinon à toute forme de recherche scientifique. Manifestement, les données préservées sur des IaaS seront conservées pendant une période de grâce après la fin du contrat avec le prestataire[565]. Cette conservation des données ne devrait pas aller au-delà de l'entente avec les tiers titulaires

---

[561] Voir Analyse de Risque, R.20 « La perte, la compromission ou l'inexistence des « journaux » d'opération et de sécurité ».
[562] LCCJTI, art. 6.
[563] Paula SAUVEUR, *La protection du secret commercial dans les nuages publics de l'infonuagique*, Cowansville, Édition Yvon Blais, mai 2013, p. 71.
[564] A. S.Y. Cheung, R. H. Weber., préc., note *488*, p. 246.
[565] Id., préc., note. 431.

de la propriété intellectuelle ou des contrats liés à l'utilisation de renseignement confidentiel, pouvant être en lien avec des données de recherche.

Somme toute, en plus d'être accentuée par la relation tripartite, nous croyons que l'obligation d'intégrité, lorsqu'il est question de données pouvant être liées aux domaines privés, impose des règles de droit importantes pouvant limiter les options d'impartition vers une IaaS. Ainsi, les risques résiduels en annexe se référant à des notions d'intégrité seront rehaussés, particulièrement pour les questions d'intégrité liée à l'entreposage, à leur traitement, à leur transfert ou à leur transport.

### 2.3.3 L'obligation d'assurer la disponibilité des données

Finalement pour ce qui est du dernier volet de la triade CID et contrairement à son affidé l'intégrité, la disponibilité est mise en exergue dans d'autres documents que la LCCJTI. Bref, il ne faut pas négliger le fait que l'obligation de disponibilité est intrinsèquement liée la localisation des données lorsque des renseignements personnels sont utilisés. À cet effet, le libellé de l'article 8 de la LPRPSP indique que :

> « **8.** La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer:
> 1° de l'objet du dossier;
> 2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise;
> 3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification. » (nos soulignements).

Il importe de soutenir à nouveau qu'il est maintenant possible pour les utilisateurs d'IaaS de choisir une région géographique dans laquelle les données pourront être conservées, mais il demeure impossible de savoir exactement la localité de ces informations. Quoi qu'il en soit, comme le soulignent certains auteurs[566], nous sommes d'avis que cette disposition devrait être revue en fonction des dossiers informatisés qui sont maintenant communément dématérialisés.

[566] J-F DE RICO, préc., note 240, p. 11.

En effet, la loi n'est pas claire quant à la définition de « l'endroit » soulevé au 3e alinéa[567]. Il pourrait être interprété comme étant un lieu physique, une ville, un pays ou voire même une région[568]. Bien entendu, la loi prévoit déjà à l'article 29, « […] l'endroit où ces dossiers sont accessibles et les moyens d'y accéder. »[569]. Donc, nous sommes d'avis que « l'endroit » prévu à l'article 8 devrait être étendu à la réalité d'aujourd'hui. Comme la commission d'accès à l'information du Québec a lancé un appel de textes pour susciter la réflexion sur l'avenir de la LPRPSP[570], nous espérons que cet article sera corrigé, ou du moins, qu'on y ajoutera une mention à cet effet.

Bien que l'université ne soit pas une entreprise privée, tel que nous l'avons vu, certains regroupements internes peuvent être assujettis aux lois de ce secteur. Ainsi, les données issues de ces liens pourront être entreposées, utilisées ou communiquées à l'extérieur du Québec moyennant « […] un examen sommaire de l'encadrement juridique du territoire visé et la conclusion d'une entente contractuelle comportant des dispositions contractuelles permettant de se confirmer aux obligations énoncées par l'article 17. »[571] à l'opposé de l'obligation imposée aux organismes publics devant prévoir une protection équivalente telle que soulignée au précédent chapitre.

Suivant ces principes, du moment où la LPRPSP exige la conclusion d'un contrat écrit,[572] il s'avère nécessaire de ne pas prendre à la légère les clauses contractuelles relatant les questions liées à la disponibilité. Elles pourront être présentes dans l'entente contractuelle avec le fournisseur de service, mais elles devront également être présentes dans le contrat unissant

---

[567] Julie M. Gauthier, « Concilier infonuagique et droit québécois », OKIOK, Avril 2014, en ligne : <https://www.okiok.com/fr/concilier-infonuagique-et-droit-defi-2/#ref21>, (consulté le 28 avril 2019)
[568] Voir Éloïse GRATTON, Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services, Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels, Les 3o ans de la Commission d'Accès à l'Information, Volume 358, Éditions Yvon Blais, Novembre 2012.
[569] LPRPSP, art. 29.
[570] Commission d'accès à l'information du Québec, « Droit d'utilisation et conditions d'utilisation », 2019, en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_Droits-auteurs_25-ans-Loi-prive.pdf>, (consulté le 28 avril 2019).
[571] Jean-François DE RICO, « La communication de renseignements personnels à l'extérieur du Québec : pour un voyage sans turbulence (art 17 de la Loi sur le secteur privé) », Développements récents : Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé, NO 392, Yvon Blais, 2014.
[572] *Deschesnes* c. *Groupe Jean Coutu (PJC) inc*., 13 juillet 2000, (C.A.I.) Commission d'accès à l'information du Québec EYB 2000-178499.

l'université avec l'acteur de l'industrie. Ces contrats, qui seront indubitablement limités dans le temps, devront encadrer ce qui découlera de la possibilité où le fournisseur de service faillira à rendre disponible l'infrastructure sous forme de service ou les données requises par le projet de recherche.

L'obligation de disponibilité est aussi encadrée par plusieurs articles de la LCCJTI auxquels nous avons déjà fait référence dans ce mémoire[573], notamment par les articles exposant les notions d'accès qui ont été rapportés sous le sujet de la confidentialité. De toute évidence, la disponibilité des documents technologiques, d'une manière plus importante que ceux traités sur des systèmes infonuagiques, devra immanquablement être contrôlée par des procédés afin de limiter leurs accès, peu importe s'ils sont liés à des organismes publics ou s'ils sont en lien avec des données liées à des intérêts privés.

Toute réflexion faite, dans le cas d'une impartition d'infrastructure universitaire vers une IaaS, la responsabilité des données traitées incombe à l'université ou plus précisément au responsable de la sécurité informationnelle. Toutefois, comme le mentionne Nicolas Vermeys, il est parfois difficile dans une organisation d'identifier ce responsable[574]. Toutefois, si les données traitées appartiennent en totalité ou en partie à une entreprise privée, les administrateurs responsables de ces données devront se conformer à la LPRPSP.

[573] LCCJTI, art. 25, art. 26; Voir notamment SECONDE PARTIE, sur l'obligation de confidentialité applicable au secteur privé.
[574] N. W. VERMEYS, préc., note 368, p.8;

# Conclusion

Entre le commencement de la recherche qui a mené à ce mémoire et l'aboutissement de sa conclusion, nous avons dû rectifier les faits sur différents aspects liés au développement de l'infonuagique, car celui-ci est en constante mouvance. Deux principaux facteurs ont mené à la nécessité d'effectuer ces changements en cours de notre rédaction: l'évolution technologique, notamment en ce qui a trait aux chiffrements, ainsi que les changements dans les contrats de service ou des licences utilisations. Nous verrons que ces deux facteurs sont aussi intrinsèquement liés aux pistes de solutions afin de permettre l'utilisation de l'infonuagique dans le système universitaire québécois.

Le premier élément ayant forcé des ajustements à ce mémoire est le développement en matière de chiffrement. Nous sommes d'avis, tel que soulevé par les auteurs de l'« étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », que :

> « […] [p]uisqu'il s'avère difficile, certains diraient même impossible, de respecter la lettre de la loi, […] 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. »[575] (nos soulignements).

Nous avons été étonnés de constater que la conclusion de cette étude, rédigée en 2014, recommandait l'utilisation du chiffrement lors du « traitement des données ». Nous croyons que la solution envisagée suggère une méthode inutilisable actuellement. C'est-à-dire que « *l'esprit de la loi* » évoqué ne saurait être totalement respecté et qu'en conséquence les données du gouvernement ne pourraient pas être portées vers les IaaS. Or comme nous l'avons vu, quoi qu'imaginé il y a plusieurs années[576], ce n'est que récemment que certains fabricants ont été en mesure d'offrir une telle possibilité qui demeure néanmoins encore restreinte[577]. Certes, d'autres

---

[575] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54.
[576] *Id*., préc., note 234.
[577] *Id.*, préc., note 235.

changements au point de vue des services infonuagiques se sont interposés pendant notre rédaction. Cela dit, l'évolution du chiffrement lors du traitement de l'information demeure un obstacle majeur afin que le passage vers l'infonuagique respecte toutes les obligations démontrées à ce mémoire.

En second lieu, bien que l'infonuagique soit issue de l'ère numérique il repose tout de même très clairement sur des bases de droit écrit : le contrat. Ces conventions infonuagiques[578] renferment des notions de gestion, de traitement des données et de fourniture d'applications logicielles. Elles invoquent aussi parfois la protection des données des utilisateurs, malgré une tendance des fournisseurs à exclure cette dernière[579]. Ces écrits sont appelés à changer au fil du temps tel que nous l'avons soulevé[580], mais pour que justice soit faite, encore faut-il que la faute soit répertoriée. Il apparaît néanmoins que les prestataires de services font preuve de mutisme. Ils privilégieront, s'il survient un bris contractuel, des arrangements à l'amiable. Ces ententes hors cour, avec les propriétaires des données, permettront d'éviter les pertes de revenus de la mauvaise publicité associées à des bris de sécurité ou à de la divulgation de renseignements confidentiels. Le gouvernement canadien a mis en vigueur le nouveau règlement portant sur la déclaration obligatoire des atteintes à la vie privée[581] en application de la loi fédérale le 1er novembre dernier[582]. Il s'agit d'un pas vers la bonne direction. À regret, aucune obligation provinciale ou sanction pécuniaire spécifique n'ont été établies par notre gouvernement, autre qu'un aide-mémoire, à l'intention des organismes et des entreprises, publié par la C.A.I. en

[578] Parfois appelées « contrat de service », contrat de « nature électronique » ou encore « contrat d'adhésion ».
[579] P. SAUVEUR, préc., note 563, p. 71.
[580] Voir notamment SECONDE PARTIE, Chapitre 1, section 1.3.3 La disponibilité, p.98; *Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île-de-Montréal* c. *Oracle Canada*, 2017 QCCS 6377.
[581] Règlement sur les atteintes aux mesures de sécurité : DORS/2018-64

[582] Alex CAMERON, Daniel FABIANO, Antoine AYLWIN et Daanish SAMADMOTEN, « Nouvelles règles importantes en matière de déclaration obligatoire d'atteinte à la vie privée et de tenue de registre au Canada », FASKEN, Avril 2018, en ligne : <https://www.fasken.com/fr/knowledgehub/2018/04/important-new-rules-for-mandatory-privacy-breach-notification>, (consulté le 28 avril 2019).

2009[583]. À contrario, le même type de protection qu'offre le Canada est offert en sol américain[584] ainsi que dans l'Union européenne[585].

Il est intéressant de noter, concernant ces accords infonuagiques, qu'il suffit d'interroger un moteur de recherche avec les termes « Microsoft Azure Agreement » pour ainsi aboutir à une version obsolète[586] des conditions d'utilisation. Ce qui pourrait rendre, à notre point de vue, ces ententes non raisonnablement accessibles vis-à-vis le C.c.Q.[587]. Néanmoins, rappelons que les versions officielles de ces conditions sont envoyées au signataire de l'entente. Nous croyons tout de même, afin de pallier cette ambiguïté, que les compagnies devraient être contraintes au maintien de leur politique à jour et au retrait des versions périmées. Elles sont actuellement trop facilement accessibles, ou du moins, les prestataires devraient clairement indiquer qu'il s'agit de versions archivées.

Dans ce mémoire, après avoir présenté les fondements théoriques de l'infonuagique[588], nous avons, au deuxième chapitre, démontré la composition des données présentes dans les universités ainsi que les obligations liées à ces données. Comme nous l'avons abordé dans la deuxième partie, les obligations, découlant des lois applicables aux institutions publiques et de celles spécifiques au secteur privé, peuvent s'appliquer à certaines catégories d'informations présentes à même nos institutions. Ces lois sont, sans équivoques, des bases à respecter pour permettre la migration et le traitement de données dans des IaaS.

Compte tenu de la rapidité d'évolution des TI, il existe des défis majeurs pour le juriste. Nous croyons néanmoins que le législateur, avec la mise en place de la LCCJTI, a su élaborer un cadre juridique adéquat afin d'établir les obligations découlant de l'utilisation des documents

---

[583] C.A.I., « Aide-mémoire à l'attention des organismes et des entreprises » en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf>, (consulté le 28 avril 2019).
[584] National Conference of State Legislature, «Security Breach Notification Laws» 29 septembre 2018, en ligne : <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>, (consulté le 28 avril 2019).
[585] *RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 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, et abrogeant la directive 5/46/CE (règlement général sur la protection des données), Journal officiel no L 119/1 du 1.5.2016.*
[586] Effectivement la recherche « Microsoft Azure Agreement » sur Google indique comme premier résultat l'accord de novembre 2014, qui n'est plus en vigueur.
[587] C.c.Q., art 1435.
[588] PREMIÈRE PARTIE, Chapitre I. Définir l'infonuagique.

technologiques. Selon notre analyse, la LCCJTI, combinée à *la Loi sur l'accès* ou la LPRPSP*,* autoriserait l'hébergement, mais pas le traitement de l'information confidentielle et des données à accès restreint chez des fournisseurs étrangers situés en sol canadien.

Le professeur Nicolas W. Vermeys a évoqué récemment quelques possibilités[589] si l'état entreprend à « transférer […] ses données à des services d'hébergement en ligne privé »[590]. Nous reprendrons trois de ses hypothèses, plus spécifiquement d'un point de vue universitaire.

Le premier scénario est le statu quo. Nous croyons que la situation des ressources informatiques des universités n'est pas aussi mal en point que celle des autres organismes gouvernementaux[591]. Néanmoins, il n'y a pas, à l'heure actuelle, de politiques sur l'utilisation des IaaS, ou concernant les autres modèles de prestation de service, dans toutes les universités. Cette situation se doit d'être corrigée[592]. L'inexistence de ces règlements a pour effet de décentraliser davantage les données issues des universités. Certains administrateurs et/ou professeurs adhèrent eux-mêmes[593] à des services infonuagiques sans valider les questions liées aux obligations de sécurité soulevées dans ce mémoire. Il est donc impératif que les universités règlementent ces questions.

En second lieu, l'utilisation du service de courtage en infonuagique du Centre de services partagés du Québec (CSPQ) est préconisée. Ce dernier précise que :

> « Dans le volet « Infrastructure » de son architecture d'entreprise gouvernementale, le Secrétariat du Conseil du Trésor (SCT) demande aux

---

[589] N. W. VERMEYS, table ronde lors de l'émission « Faut pas croire tout ce qu'on dit » au cours de l'épisode intitulé : « Le Québec entend confier au privé les données personnelles qu'il détient sur ces citoyens » (9 février 2019).
[590] Id., préc., note 5.
[591] Les virus EMOTET, reconnu comme étant particulièrement difficile à éradiquer, et QAKBOT, on récemment (mars 2019) mis hors services des postes de travail du ministère de l'Énergie et des Ressources naturelles (à l'exception du Registre foncier du Québec), du ministère des Forêts, de la Faune et des Parcs et de Transition énergétique Québec. Afin d'éviter toute propagation et, par mesure préventive, les postes de travail visés ont été fermés. Aucunes données n'auraient néanmoins été affectées.
[592] Nous devons saluer ici la directive concernant le stockage de l'information institutionnelle en infonuagique de l'Université de Montréal, pré., note 191; Malheureusement, cette politique fait référence seulement au stockage de l'information et non au IaaS.
[593] Notons ici que les fonds du CRSNG ne peuvent pas être utilisé pour adhérer à des services infonuagique. Voir à notamment CRSNG, « Utilisation des subventions », 5 octobre 2017, en ligne : <http://www.nserc-crsng.gc.ca/Professors-Professeurs/FinancialAdminGuide-GuideAdminFinancier/FundsUse-UtilisationSubventions_fra.asp>, (consulté le 28 avril 2019).

> organismes publics de recourir au Catalogue pour trouver une ou des offres qui répondent à leurs besoins et qui correspondent à leur analyse de risques. »[594].

Encore faut-il que les universités aient un responsable de la sécurité informationnelle et que ce dernier ait établi une analyse des risques à jour. Nous croyons que ce scénario vise aussi à mener les chercheurs universitaires vers des modèles communautaires[595] québécois. En effet, Calcul Canada et CMC Microsystems, pour nommer que ceux-ci, offrent certains services d'infrastructures sous forme de service limité[596]. Cependant, il nous apparaît illogique de pouvoir obtenir des services d'IaaS semblables offerts par deux joueurs différents financés tous les deux par le gouvernement[597]. Pourtant la politique de la FCI est claire et sans équivoque[598] comme indiqué en début de seconde partie. Rappelons que Microsoft, par exemple, investit l'équivalent d'un tiers du budget du Québec[599]. C'est pourquoi il vaut mieux liguer les deniers publics chez un seul fournisseur de services infonuagiques de recherche universitaire afin d'obtenir une sécurité comparable, ou du moins raisonnable.

En dernier lieu, il s'agirait d'adhérer au nuage public tout en limitant l'hébergement et le traitement des données au Québec, ou du moins au Canada. Cette option répond aux requis de la *Loi sur l'accès*[600] et de la LPRPSP[601]. Ainsi, il ne resterait plus que la question du USA Cloud Act américain, puisque, même s'il est situé au Québec, les données seraient en main de sociétés étrangères. Une échappatoire existe au Cloud Act. Il serait donc possible pour le Canada de conclure un accord bilatéral permettant des échanges d'informations ne ciblant que les

---

[594] CSPQ, « Guide de l'Utilisateur, Catalogue d'offres infonuagique », en ligne < http://www.portail.approvisionnement-quebec.gouv.qc.ca/fileadmin/Documents/PDF/guide_utilisateur_courtier_infonuagique.pdf>, (consulté le 28 avril 2018).

[595] Voir PREMIÈRE PARTIE, chap. 1, section 1.3.3 Le modèle communautaire.

[596] Par service limité, nous entendons : des limites dans les ressources, des limites du temps d'utilisations, etc.

[597] Id., préc., note 335 (Calcul Canada reçoit 572.5M, offre un service d'IaaS); et CMC Microsystem, « Canada's National Design Network »., reçoit 8.08M, notamment pour offrir un service d'IaaS. Voir « list of funded projects en ligne : <https://www.innovation.ca/sites/default/files/database_download/march2019/list_of_awards_for_web.xlsx>, (consulté le 28 avril 2019).

[598] *Id*., préc., note 337, p. 77.

[599] Voir notamment Ridha LOUKIL, « Les cinq chiffres clés du cloud de Microsoft en 2018 », *L'UsineNouvelle*, (3 février 2019), en ligne : <https://www.usinenouvelle.com/article/les-quatre-chiffres-cles-du-cloud-de-microsoft-en-2018.N801215>; et Finance Québec, « Le Québec en quelques chiffres », Mars 2017, en ligne : <http://www.budget.finances.gouv.qc.ca/quebec-en-chiffres/index201703.html#.>, (consulté le 28 avril 2019).

[600] *Loi sur l'accès*, art. 70.1.

[601] LPRPSP, art. 17.

citoyens américains[602]. Certes, la problématique serait reconduite advenant qu'un citoyen ait une double nationalité. Il s'agirait là, encore une fois, d'une amélioration à l'égard de la situation actuelle.

Dans le but de répondre aux obligations traitées dans ce mémoire, il faudrait, bien entendu, que le chiffrement lors du traitement des données soit possible. Spécifions que nous serons toujours tributaires des changements technologiques ou législatifs pour veiller à la sécurité de nos informations. Prenons pour exemple le gouvernement australien qui a adopté un controversé projet de loi[603], à l'intérieur duquel il oblige les entreprises de technologie à fournir un moyen détourné « backdoor[604] » afin de permettre aux agences de sécurité d'accéder aux communications chiffrées.

Nous croyons, somme toute, que le passage vers l'infonuagique est inévitable. Ne serait-ce qu'en support aux infrastructures universitaires déjà imposantes. Il est reconnu que la plupart des passages vers des IaaS peuvent se faire de manière ataraxique. Après tout, l'IaaS à l'étude est le modèle infonuagique offrant le plus de contrôle par l'université.

> « […] l'organisation cliente possède un droit de regard sur la configuration du système et dispose ainsi d'un plus grand contrôle sur celui-ci. »[605].

Les règlements des universités devraient circonscrire l'utilisation des catégories de données confidentielles et à accès restreint au traitement sur les systèmes infonuagiques, du moins jusqu'à ce qu'il soit possible de traiter des données chiffrées.

Finalement, ce n'est pas parce qu'on garde de l'information à l'interne que c'est d'entrée de jeu plus sécuritaire. Dans le cas où les expertises et les mesures de sécurité adéquates ne sont

---

602 Vincent HERMANN, «Cloud Act : l'accès aux données extraterritoriales « clarifié » aux États-Unis, mais critiqué », 26 mars 2018, en ligne <https://www.nextinpact.com/news/106367-cloud-act-lacces-aux-donnees-extraterritoriales-clarifie-auxetats-unis-mais-critique.htm>, (consulté le 28 avril 2019).

603 Jamis TARABAY, « Australian Government Passes Contentious Encryption Law », *NY Times*, Décembre 2018, en ligne : <https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html>, (consulté le 28 avril 2019).

604 OQLF., préc., note 10, « backdoor » : « Porte d'accès à un programme ou à un système d'exploitation, prévue pour les tests et la maintenance, permettant le contournement des mécanismes de sécurité et qui, de ce fait, en rend la pénétration possible par un pirate l'ayant découverte. ».

605 Voir notamment : N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 161; W. Kuan HON, Christopher MILLARD et Ian WALDEN, « Negotiating Cloud Contracts: Looking at Clouds from Bothsides Now », (2012) 16 *Stan. Tech. L. Rev.* 81, 617.

pas au rendez-vous, il sera possiblement plus sécuritaire de conserver ou traiter les données à l'extérieur des murs de l'université.

Dans l'affaire *Chambre de l'assurance de dommage* c. *Kotliaroff*, il a été mentionné :

> « Il est probable que le recours au service d'une entreprise spécialisée dans la création de site web aurait permis à l'intimé d'éviter le bris de confidentialité qui lui est, aujourd'hui, reproché dans la présente plainte; »[606]

Autrement dit, traiter avec des compagnies spécialisées peut parfois atténuer des risques importants. Ajoutons également que:

> «*Cloud computing does not necessarily create challenges that you do not already face with locally installed technology. The biggest difference is that you may not have had to worry about these challenges before. Placing your information in the cloud makes addressing these challenges an imperative.* » [607].

Comme les TI évoluent beaucoup plus rapidement que le droit, comment pourrions-nous dénicher une parfaite conclusion ? Peut-être vivrons-nous bientôt un prochain cycle de décentralisation[608]? En définitive, il serait primordial de conserver le contrôle sur nos données et ainsi maintenir une souveraineté numérique, car après tout :

*scientia potentia est*.[609]

---

[606] *Chambre de l'assurance de dommages* c. *Kotliaroff*, 2008 QCCDCHAD 19078.
[607] D. P. WHELAN, préc., note 259 p. 27.
[608] Par exemple : L'informatique quantique pourrait, semble-t-il, augmenter significativement la vitesse de calcul, ce qui résulterait en une une facilité accrue et de meilleurs niveaux du chiffrement. Voir notamment, Joël Leblanc, « L'ordinateur quantique mettra l'internet K.O. » *Québec science*, 26 novembre 2016, en ligne : <https://www.quebecscience.qc.ca/technologie/lordinateur-quantique-mettra-linternet-k-o/>, (consulté le 28 avril 2019).
[609] Locution latine que l'on peut traduire par "*Le savoir, c'est le pouvoir*", généralement attribué au philosophe Francis Bacon.

# Table de la Législation

*Textes fédéraux*

*Code criminel*, L.R.C. (1985), c. C-46.

*Loi sur l'accès à l'information*, L.R.C. (1985), c. A-1.

*Loi sur la protection des renseignements personnels et documents électroniques*, L.C. (2000), c. 5.

*Loi sur le droit d'auteur*, L.R.C. 1985, c C-42.

Loi sur les brevets L.R.C. (1985), ch. P-4

*Loi sur les télécommunications,* L.e. 1993, c. 38.

*Règlement sur les signatures électroniques sécurisées DORS/2005-30*

*Règlement sur les atteintes aux mesures de sécurité : DORS/2018-64*

*Textes québécois*

*Code civil du Québec*, L.Q. 1991, c. 64.

*Code des professions,* L.R.Q. c. C-26.

*Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1.

*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* L.R.Q. c. A-2.1.

*Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement*, L.R.Q., c. G-1.03.

*Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., ch. P-39.1.

*Loi sur la sécurité civile,* L.R.Q., c. S-2.3.

*Loi sur les archives,* L.R.Q. c. A-21.1.

*Règlement sur les atteintes aux mesures de sécurité, DORS/2018-64.*

*Règlement sur les contrats du Protecteur du citoyen, RLRQ c P-32, r 2.*

*Textes et instruments étrangers et internationaux*

*Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712)*

*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,* PUBLIC LAW 107-56, 115 Stat. 272.

*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, PUBLIC LAW 114-23, 129 STAT. 268*

*RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 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, et abrogeant la directive 5/46/CE (règlement général sur la protection des données), Journal officiel n$^{o}$ L 119/1 du 1.5.2016.*

# Table de la jurisprudence

*Jurisprudence canadienne*

## *Jurisprudence américaine*

# Bibliographie

*Monographies et ouvrages collectifs*


ACKERMANN, T., *IT Security Risk Management*, Springer Gable, 2013.

BASIN, D., P. SCHALLER et M. SCHLÄPFER, *Applied Information Security- A Hands-on Approach*, Springer, Berlin, Heidelberg, 2011.

BATINI, C. et M. SCANNAPIECO, *Data and Information Quality, Dimensions, Principles and Techniques*, Switzerland, Springer, 2016.

BENYEKHLEF. K., *Une possible histoire de la norme, Les normativités émergentes de la mondialisation*, Montréal, Thémis, 2008.

BUYYA, R., J. BROBERG et A.-M. GOSCINSKI, *Cloud Computing Principles and Paradigms*, Hoboken Wiley, 2011.

CHEUNG, A. S.Y. et R. H. WEBER, *Privacy and legal issues in cloud computing*, Cheltenham, Edward Elgar Publishing, 2016.

CÔTÉ, P.-A*., Interprétation des lois*, 4e éd., Montréal, Les Éditions Thémis, 2009.

CRÉPEAU, P-A., *L'intensité de l'obligation juridique*, Cowansville, Éditions Yvons Blais, 1989.

DORAY, R. et F. CHARETTE, *Accès à l'information : loi annotée, jurisprudence, analyse et commentaires*, Cowansville, Yvon Blais, 2001.

DORAY, R. et F. CHARRETTE, *Accès à l'information*, Cowansville, Éditions Yvon Blais, 2013.

ELTIS K., *Courts, Litigants and the Digital Age: Law, Ethics and Practice*, Toronto: Irwin Law, 2012

GAUTRAIS, V. et P. TRUDEL, *Circulation des renseignements personnels et web 2.0*, Montréal, Éditions Thémis, 2010.

GRANOSIK, L. et K-A. GRENIER, *La Loi sur la protection des renseignements personnels dans le secteur privé : 2e édition annotée*, Cowansville, Édition Yvon Blais, 2013.

GRATTON, É., *Understanding Personal Information*, Managing Privacy Risks, Markham, LexisNexis, 2013.

GUTWIRTH, S. *et al*., eds, *Reinventing Data Protection?,* London, Springer, 2009.

HANSCHE, S., *et al*., *Official (ISC)2 Guide to CISSP Exam*, Boca Raton, Auerbach, 2004.

HILL R., L. HIRSCH, P. LAKE et S. MOSHIRI, *Guide to Cloud, Principles and Practice*, London, Springer, 2013.

HUBIN, J. et Y. POULLET, *La sécurité informatique, entre technique et droit*, Namur C.R.I.D., 1998.

MILLARD, C., *Cloud Computing Law*, Oxford, Oxford University Press, 2014.

MURUGESAN, S. et I. BOJANOVA, *Encyclopedia of Cloud Computing*, Chichester, Wiley-IEEE Press, 2016.

PEARSON, S. et G. YEE, *Privacy and Security for Cloud Computing*, London, Springer, 2013.

SAMANI, R., J. REAVIS et B. HONAN, *CSA Guide to Cloud Computing, Implementing Cloud Privacy and Security*, Waltham, Syngress, 2014.

SAUVEUR, P., *La protection du secret commercial dans les nuages publics de l'infonuagique*, Cowansville, Édition Yvon Blais, mai 2013.

SOSINSKY, B., *Cloud Computing Bible*, Indianapolis, Wiley, 2011.

TIPTON, H.F. et K. HENRY (éds), *Official (ISC)$^2$ Guide to the CISSP CBK*, Boca Raton, Auerbach Publications, 2007.

TRUDEL, P., F. ABRAN, K. BENYEKHLEF et S. HEIN, *Droit du cyberespace*, Montréal, Thémis, 1997.

VERMEYS, N. W., *Droit codifié et nouvelles technologies : le Code civil*, Montréal, Éditions Yvon Blais, 2015.

VERMEYS, N. W., *Responsabilité civile et sécurité informationnelle*, Cowansville, Éditions Yvon Blais, 2010

WHELAN, D. P., *Practice Law in the Cloud*, Aurora, Canada Law book, 2013

*Articles de revue et études d'ouvrages collectifs*

BENYKHLEF, K., J. BAILEY, J. BURKELL, et F. GÉLINAS, « eAccess to Justice », University of Ottawa Press 2016, en ligne : < https://commentary.canlii.org/w/canlii/2016CanLIIDocs415.pdf>.

BICH, M.-F., « Emploi et propriété intellectuelle – médiation sur les droits moraux du salarié », *Journal du Barreau du Québec*, Volume 31 numéro 20, 1999.

CASSIUS DE LINVAL, R., « Loi concernant le cadre juridique des technologies de l'information, Une innovation législative majeure » *Journal du Barreau du Québec*, Volume 33 numéro 17, 2001.

CHANDLER, J. A., «Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software. SECURING PRIVACY IN THE INTERNET AGE», *Stanford University Press*, 2006. En ligne : <https://ssrn.com/abstract=610041>.

CHANDLER, J. A. «Security in Cyberspace: Combatting, Distributed Denial of Service Attacks», *University of Ottawa Law & Technology Journal*, Vol. 1, p. 231, 2003-2004.

COCHRAN, M. et P. D. WITMAN, « Gouvernance and service level agreement issues in a cloud computing environment », *Journal of Information Technology Management*, Volume XXII, Number 2, 2011 en ligne : <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.6370&rep=rep1&type=pdf>.

DE RICO, J.-F., « L'infonuagique, la protection des renseignements personnels et les droits d'accès des gouvernements », (2014) 6 *Technologies de l'information en bref.*

DE RICO, J.-F., « La communication de renseignements personnels à l'extérieur du Québec : pour un voyage sans turbulence (art 17 de la Loi sur le secteur privé) », Développements récents : Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé, NO 392, Yvon Blais, 2014.

GRATTON, É., « Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services », *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels, Les 30 ans de la Commission d'Accès à l'Information*, Volume 358, Éditions Yvon Blais, Novembre 2012.

MUNIER, M., V. LALANNE, P.-Y. ARDOY et M. RICARDE, *Métadonnées & Aspects juridiques Vie Privée vs Sécurité de l'Information,* 9ème Conférence sur la Sécurité des Architectures Réseaux et des Systémes d'Information (SARSSI'2014), May 2014, Saint-Germain-Au-Mont-d'Or, France.

PEAK, D. A., et M. H. AZADMANESH, « Centralization/decentralization cycles in computing: Market evidence. », 1997 *Information and Management* 31(6), 303–317.

R. BALASUBRAMANIAN, M. ARAMUDHAN, « Security Issues: Public vs Private vs Hybrid Cloud Computing», *International Journal of Computer Applications*, volume 55- No.13, Octobre 2012 p. 37.

ROUSSEL G. (dir.), Autoroute de l'information en droit d'auteur : collision ou covoiturage, (Actes de la journée d'étude tenue à Montréal, le 18 novembre 1994), Montréal, ALAI-Canada.

ROUSSEL, G., « La gestion de la propriété intellectuelle dans les relations entre l'université et l'entreprise : pour une véritable dynamique d'alliances stratégiques; ; Propriété intellectuelle et université – entre la libre circulation des idées et la privatisation des savoirs ; Université inc. – des mythes sur la hausse des frais de scolarité et l'économie du savoir », *Les cahiers de propriété intellectuelle*, 2012, en ligne : <https://cpi.openum.ca/files/sites/66/Propriété-intellectuelle-et-université.pdf>.

SOLMECKE C., «The Legal Aspect of cloud Computing under Copyright Law», *Wilde Beuger Solmecke*, (13 septembre 2013), en ligne : <https://www.wbs-law.de/eng/it-law/the-legal-aspects-of-cloud-computing-under-copyright-law-45886/>.

TRUDEL, P. et F. ABRAN, « Guide sur la protection de la vie privée dans les services de courrier électronique en site web », Chaire L.R. Wilson sur le droit des TI et du Commerce Électronique, CRDP. 24 octobre 2000, en ligne : <http://pierretrudel.chairelrwilson.ca/pdf/courrier_site_web.pdf>.

TRUDEL P., « Privacy Protection on the Internet: Risk Management and Networked Normativity» dans Serge Gutwirth *et al*., eds, *Reinventing Data Protection? (Dordrecht, London: Springer, 2009).*

TRUDEL, P, F. ABRAN, G. DUPUIS, « Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions », Rapport préparé pour la Direction des politiques du ministère des services gouvernementaux du Québec (Montréal : chaire L.R. Wilson et CRDP, 2007).

VERMEYS, N. W., J, M. GAUTHIER et S. MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », Centre de recherche en droit public, Université de Montréal, mars 2014.

W. Kuan HON, Christopher MILLARD et Ian WALDEN, « Negotiating Cloud Contracts: Looking at Clouds from Bothsides Now », (2012) 16 *Stan. Tech. L. Rev.* 81.

*Documents gouvernementaux*

CAI, « La gestion des renseignements personnels dans les universités et cégeps », (1995), en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_FI_rens_pers_univ-cegep.pdf>.

CAI, « Qu'est ce qu'un renseignements personnel ? », en ligne : <http://www.cai.gouv.qc.ca/citoyens/acces-et-protection-de-vos-renseignements-personnels/quest-ce-quun-renseignement-personnel/>.

CAI, « Aide-mémoire à l'attention des organismes et des entreprises » 7 avril 2009, en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf>.

CAI, « Droit d'utilisation et conditions d'utilisation », 2019, en ligne : <http://www.cai.gouv.qc.ca/documents/CAI_Droits-auteurs_25-ans-Loi-prive.pdf>,

COMMISSION DE L'ÉTHIQUE, DE LA SCIENCE ET DE LA TECHNOLOGIE, « Viser un juste équilibre, Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité », Avis adopté à la 34e réunion de la Commission, 12 février 2008.

CONSEIL DE LA SCIENCE ET DE LA TECHNOLOGIE, « La gestion de la propriété intellectuelle dans les relations entre l'université et l'entreprise : pour une véritable dynamique d'alliances stratégiques », Ministère du Développement économique, de l'innocation et de l'Exportation, 2011, en ligne : < http://collections.banq.qc.ca/ark:/52327/bs2103875>.

CREPUQ, « Recueil des règles de conservation des documents des établissements universitaires québécois (édition électronique à jour le 30 mai 2002) », Montréal, en ligne : <https://www.bci-qc.ca/wp-content/uploads/2017/05/Recueil-regles-conservation-CREPUQ.pdf>.

CRSNG, « Utilisation des subventions », (5 octobre 2017), en ligne : <http://www.nserc-crsng.gc.ca/Professors-Professeurs/FinancialAdminGuide-GuideAdminFinancier/FundsUse-UtilisationSubventions_fra.asp>.

CSPQ, en ligne : <https://www.cspq.gouv.qc.ca/>.

CSPQ, « Guide de l'Utilisateur, Catalogue d'offres infonuagique », (28 novembre 2018), en ligne <http://www.portail.approvisionnement-quebec.gouv.qc.ca/fileadmin/Documents/PDF/guide_utilisateur_courtier_infonuagique.pdf>

C.V.P.C., « Comment réagir à une atteinte à la vie privée dans votre entreprise » Novembre 2018, en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/atteintes-a-la-vie-privee/comment-reagir-a-une-atteinte-a-la-vie-privee-dans-votre-entreprise/gd_pb_201810/>.

FINANCE QUÉBEC, « Le Québec en quelques chiffres », Mars 2017, en ligne : <http://www.budget.finances.gouv.qc.ca/quebec-en-chiffres/index201703.html#>.

FONDATION CANADIENNE POUR L'INNOVATION, « Guide des politiques et des programmes, 2017 » en ligne : <https://www.innovation.ca/sites/default/files/essential_documents/guide_des_politiques_et_des_programmes_de_la_fci-sommaire_des_principales_modifications_2017.pdf.>

FONDATION CANADIENNE POUR L'INNOVATION « list of funded projects », mars 2019, en ligne : <https://www.innovation.ca/sites/default/files/database_download/march2019/list_of_awards_for_web.xlsx>.

GOUVERNEMENT DU CANADA, « Déclaration de principes des trois organismes sur la gestion des données numériques », en ligne <http://www.science.gc.ca/eic/site/063.nsf/fra/h_83F7624E.html?OpenDocument>.

GOUVERNEMENT DU CANADA, « Protéger votre numéro d'assurance sociale », (18 juillet 2018), en ligne : <https://www.canada.ca/fr/emploi-developpement-social/programmes/numero-assurance-sociale/proteger.html>.

GOUVERNEMENT DU QUÉBEC, MERN - Ministère de l'Énergie et des Ressources naturelles du Québec, (mai 2015), en ligne : <https://www.mern.gouv.qc.ca/publications/ministere/politique/securite-information.pdf>

GOUVERNEMENT DU QUÉBEC, Secrétariat du Conseil du trésor du Québec, « Volet Infrastructures, Énoncés d'orientation en infonuagique, Architecture d'entreprise gouvernementale 3.2 », (Mai 2016), en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG_3_2/Enonces_orientation_infonuagique.pdf>

GOUVERNEMENT DU QUÉBEC, Conseil du Trésor, « Cadre gouvernemental de gestion – Sécurité de l'information », (Juin 2014), en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_securite_information.pdf>

GROUPE CONSULTATIF INTERORGANISME EN ÉTHIQUE DE LA RECHERCHE, « Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains », Chapitre 3 – Vie privée et confidentialité des données, en ligne : < http://www.ger.ethique.gc.ca/archives/tcps-eptc/docs/TCPSsec03f.pdf>.

MORNEAU W. F., Ministre des Finance, « Égalité Croissance, une classe moyenne forte », (Février 2018), en ligne : <https://www.budget.gc.ca/2018/docs/plan/budget-2018-fr.pdf.>

MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX, « *Plan de classification uniforme des documents du MSSS*, Santé et Services sociaux », Février 2011.

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR, DE LA RECHERCHE, DE LA SCIENCE ET DE LA TECHNOLOGIE, « plan de classification des documents du ministères de l'Enseignement supérieur, de la Recherche, de la Science et de la Technologie », Septembre 2013.

MINISTÈRE DE L'ÉDUCATION ET DE L'ENSEIGNEMENT SUPÉRIEUR, « Rapport Annuels de l'Université du Québec et de ses établissements », en ligne : < https://www.uquebec.ca/reseau/fr/publications/rapports-annuels>.

SECRETARIAT DU CONSEIL DU TRÉSOR DU CANADA, « Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : Mise à jour de 2018 », en ligne : <https://www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/informatique-nuage/profil-controle-securite-services-ti-fondes-information-nuage.html>.

SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, « Nouveau portail pour les données ouvertes – Favoriser l'innovation et la diffusion d'information », *CNW Telbec*, 5 avril 2016, en ligne <http://www.fil-information.gouv.qc.ca/Pages/Article.aspx?aiguillage=diffuseurs&type=1&listeDiff=4&idArticle=2404057570>.

SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, « Volet Infrastructures, Énoncés d'orientation en infonuagique, Architecture d'entreprise gouvernementale 3.2 », Mai 2016, en ligne : <https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG_3_2/Enonces_orientation_infonuagique.pdf>.

SECRÉTARIAT DU CONSEIL DU TRÉSOR DU QUÉBEC, « Volet Infrastructures, Guide de l'infonuagique, Architecture d'entreprise gouvernementale 3.0 », Octobre 2014, en ligne : < https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/architecture_entreprise_gouvernementale/AEG30_Infonuagique_v4_GestionContractuelle_accessible.pdf>.

*Dictionnaires et ouvrages de références*

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Le grand dictionnaire terminologique », en ligne : <http://www.granddictionnaire.com/index.aspx>.

## LITTÉRATURE TECHNIQUE

ARCHER, J. *et al*., « Security Guidance for critical areas of focus in cloud computing v.3.0», CSA, 2011, en ligne : <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf>.

BAUDOIN., C. *et al*., Cloud Standards Customer council, «Cloud Security Standards: What to Except & What to Negociate, Version 2.0», Août 2016.

CULLENS, C. *et al*., « Always Encrypted with Secure Enclaves », Microsoft Corporation, SQL Docs, 23 Septembre 2018.

CLOUD SECURITY ALLIANCE, «SecaaS Implementation Guidance, Category 8: Encryption», Septembre 2012, en ligne : <https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf>.

DARA S., « Cryptography Challenges for Computational Privacy in Public Clouds », International Institute of Information Technology, 2013, en ligne : <https://eprint.iacr.org/2013/272.pdf>.

ENISA, « Cloud Computing, Benefits, risks and recommendations for information security », Novembre 2009; Sailesh GADIA, « Cloud Computing Risk Assessment, A Case Study», ISACA Journal, Volume 4, 2011.

JANSEN, W. et T. GRANCE, « Guidelines on Security and Privacy in Public Cloud Computing », NIST, Décembre 2011, en ligne : <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf >.

KENT, K., et M. SOUPPAYA, NIST, *Guide to Computer Security Log Management,* SP 800-92, Special Publication, Septembre 2016.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*, Guide for Conducting Risk assessments*, SP 800-30 Revision 1, 2012, chapitre 2 page 5, en ligne : <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

Norme ISO/IEC 31000 :2018, « Management du risque », Organisation Internationale de Normalisation (ISO), Genève, 2018.

Norme ISO/IEC 27005 :2008, « Technologies de l'information -- Techniques de sécurité -- Gestion des risques en sécurité de l'information », Organisation Internationale de Normalisation (ISO), Genève, 2008.

Norme ISO/IEC 19086-2016, « Cloud Service Level Agreement standardisation guidelines », Organisation Internationale de Normalisation (ISO), Genève.

Norme ISO/IEC 27018:2014, « Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII », Organisation Internationale de Normalisation (ISO), Genève.

Norme ISO/IEC 27017:2015, « Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage », Organisation Internationale de Normalisation (ISO), Genève.

Norme ISO/IEC 27002:2013 « Information technology – Security techniques – Code of pratice for information security controls », Organisation Internationale de Normalisation (ISO), Genève.

ORGANISATION INTERNATIONALE DE NORMALISATION, ISO/IEC 27018:2014, « Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII », 2014, Genève.

SAHAI, A. « Computing on Encrypted Data » (2008), *International Conference on Information Systems Security.*

SALEH, E., A. ALSA'DEH, A. KAYED et C. MEINEL « Processing over encrypted Data : Between Theory and Practice » SIGMOD Record, September 2016 (Vol. 45, No. 3).

## RESSOURCES ÉLECTRONIQUES ET ARTICLES DE JOURNAUX


ALDIAB, M., « Public Cloud War: AWS vs Azure vs Google », *Cloud Academy*, en ligne < https://cloudacademy.com/blog/public-cloud-war-aws-vs-azure-vs-google/>.

AMAZON WEB SERVICES, « Amazon Compute Service Level Agreement », 12 Février 2018, en ligne : < https://aws.amazon.com/compute/sla/>.

AMAZON WEB SERVICES, «Amazon Information Request Reports », <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF >.

AMAZON WEB SERVICES, « Localisation des données Perspectives de la stratégie AWS », Juillet 2018, en ligne : <https://d1.awsstatic.com/whitepapers/compliance/FR_Whitepapers/Data_Residency_Whitepaper.pdf>.

ANSYS « Software License Agreement », 28 décembre 2018, en ligne : < https://www.ansys.com/-/media/ansys/corporate/files/pdf/footer/wla-december-28-2018.pdf?la=en>.

BADGER, L., T. GRANCE, R. PATT-CORNER et J. VOAS, « Cloud computing synopsis and recommendations », NIST, Mai 2012, en ligne : < https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>.

BALDWIN, M., « Azure Disk Encryption for Windows and Linux IaaS VMs », Microsoft Corporation, 15 mars 2019, en ligne : <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption>.

BARLOW, J., « La course aux étudiants étrangers », *L'actualité*, 9 février 2018, en ligne : <https://lactualite.com/societe/la-course-aux-etudiants-etrangers/>.

BERGEN, M., « Google Will Stop Reading Your Emails for Gmail Ads », *Bloomberg*, (23 June 2017), en ligne : <https://www.bloomberg.com/news/articles/2017-06-23/google-will-stop-reading-your-emails-for-gmail-ads>.

CALCUL CANADA, « compute canada applauds $572.5 million investment in digital research infrastructure », Février 2018, en ligne : <https://www.computecanada.ca/featured/compute-canadas-applauds-572-5-million-investment-in-digital-research-infrastructure/>.

CALCUL CANADA, « L'infonuagique pour les chercheurs », (Décembre 2016), en ligne : <https://www.computecanada.ca/wp-content/uploads/2015/03/CloudStrategy2016-2019-forresearchersEXTERNALFrCa.docx.pdf>.

CALCUL CANADA, « Research Portal », en ligne : <https://www.computecanada.ca/page-daccueil-du-portail-de-recherche/acces-aux-ressources/glossaire-technique/?lang=fr>.

CAMERON, A., D. FABIANO, A. AYLWIN et D. SAMADMOTEN, « Nouvelles règles importantes en matière de déclaration obligatoire d'atteinte à la vie privée et de tenue de registre au Canada », *FASKEN*, Avril 2018, en ligne : <https://www.fasken.com/fr/knowledgehub/2018/04/important-new-rules-for-mandatory-privacy-breach-notification>.

CANADIAN ASSOCIATION FOR GRADUATE STUDIES, « A Guide to Intellectual Property », en ligne : <http://www.cags.ca/documents/publications/working/Guide_Intellectual_Property.pdf>.

CHAMBRE DE COMMERCE DU MONTRÉAL MÉTROPOLITAIN, « La collaboration universités-entreprises : le regard des centres et chaires de recherche », 2012, en ligne : <https://www.ccmm.ca/documents/pdf/RDVS-Savoir2012_fr.pdf>.

COPIBEC, « Saviez-vous que vous détenez les droits d'auteur sur vos travaux scolaires? », 11 Avril 2018, en ligne : <https://www.copibec.ca/fr/nouvelle/165/saviez-vous-que-vous-detenez-les-droits-d-auteur-sur-vos-travaux-scolaires>.

DELWAIDE, K., « Protection de l'information et de la vie privée », *FASKEN*, 2006, en ligne < https://www.fasken.com/fr/solution/practice/privacy-and-cybersecurity#sort=%40fclientworksortdate75392%20descending>.

FÉDÉRATION QUÉBÉCOISE DES PROFESSEURES ET PROFESSEURS D'UNIVERSITÉ, « The funding of University Research in Quebec : Evolution and Challenge », Abstract, Février 2016. En ligne : <http://fqppu.org/le-financement-de-la-recherche-universitaire-au-quebec-evolution-et-enjeux/>.

FELDER, T., « SaaS : Single Tenant vs Multi-Tenant – What's the Difference? », *DataInsider Digital Guardian's Blog*, 26 Avril 2019, en ligne : <https://digitalguardian.com/blog/saas-single-tenant-vs-multi-tenant-whats-difference>.

GALLAGHER, P. J. «The CLOUD Act: Mooting the Microsoft Ireland Case, but not forecasting clear skies just yet. », *Columbia Business Law Review*, 13 Avril 2018, en ligne : <https://cblr.columbia.edu/the-cloud-act-mooting-the-microsoft-ireland-case-but-not-forecasting-clear-skies-just-yet/>.

GAUTHIER, J. M., « Concilier infonuagique et droit québécois » *OKIOK*, (Avril 2014), en ligne : <https://www.okiok.com/fr/concilier-infonuagique-et-droit-defi-2/#ref21>.

GIRARD, G. et C. GRONDIN, « Le financement des universités, Historique, explications et recommandations pour une nouvelle formule de financement », Union Étudiante du Québec, 2017.

GOOGLE, « Digital Security & Due Process: Modernizing Cross Border Government Access Standards for the Cloud Era » en ligne : <https://blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf>.

GOOGLE, « Google Compute Engine Service Level Agreement », en ligne : < https://cloud.google.com/compute/sla>.

GOOGLE, « Google Transparency report », en ligne : <https://transparencyreport.google.com/user-data/overview>.

GOOGLE CLOUD DOCUMENTATION, « suppression des données sur GCP », (20 février 2019), en ligne <https://cloud.google.com/security/deletion/>.

GOYAL, S. « Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review », *I.J. Computer Network and Information Security* 2014, 3, 20-29, p. 25. en ligne : < http://www.mecs-press.org/ijcnis/ijcnis-v6-n3/IJCNIS-V6-N3-3.pdf>.

HACHMCN, M., «Microsoft's FPGA-powered supercomputers can translate wikipoedia faster than you can blink », (26 Septembre 2016), *PCWorld*, en ligne : <https://www.pcworld.com/article/3124486/hardware/microsofts-fpga-powered-supercomputer-can-translate-wikipedia-faster-than-you-can-blink.html>.

HERMANN, V., « Cloud Act : l'accès aux données extraterritoriales « clarifié » aux États-Unis, mais critiqué », *Nextinpact*, (26 mars 2018), en ligne <https://www.nextinpact.com/news/106367-cloud-act-lacces-aux-donnees-extraterritoriales-clarifie-auxetats-unis-mais-critique.htm>.

HURLEY, L., «U.S. top court rules that Microsoft email privacy dispute is moot.» *Reuters*, 17 Avril 2018, en ligne : <https://www.reuters.com/article/us-usa-court-microsoft/supreme-court-rules-that-microsoft-email-privacy-dispute-is-moot-idUSKBN1HO23S>.

INFORMATION SCIENCE INSTITUTE, University of Southern California, RFC : 793, « Transmission control protocol, protocol specification », en ligne <http://tools.ietf.org/html/rfc793>.

INSTITUT CANADIEN DES COMPTABLES AGRÉÉS, « Guide sur les normes comptables pour les organismes sans but lucratif canadiens », 2012. en ligne : <https://www.cpacanada.ca/-/media/site/business-and-accounting-resources/docs/guides-normes-comptables-osbl-sept-2012_20021.pdf?la=fr&hash=2CFAB131F906C4B2B6DA9B4A34990416C735FD1A>.

JHONSA, E., «Amazon's Spending on the Cloud is Growing, but Not Nearly as Fast as Facebook's», *TheStreet*, (Août 2018), en ligne : <https://www.thestreet.com/technology/amazons-cloud-capital-spending-is-growing-but-not-as-fast-as-facebooks-14678361>.

JUNG, D., « Québec confiera le stockage des données publiques au privé », (Février 2019) *ICI Radio-Canada*, en ligne : <https://ici.radio-canada.ca/nouvelle/1150932/centres-donnees-informatiques-cti-ibm-amazon-caire>.

KNIBBS, K., « The US House Just Voted to Stop NSA's Bulk Data Collection», *Gizmodo*, 13 mai 2015, en ligne : <https://gizmodo.com/house-committee-votes-to-reform-usa-patriot-act-with-us-1700758645>.

LAWRENCE, J., « Photos piratées de stars : Tous les utilisateurs de clouds doivent-ils être inquiets? », (19 septembre 2014), *AFP – 20 Minutes*, en ligne : <https://www.20minutes.fr/high-tech/1435971-20140902-photos-piratees-stars-tous-utilisateurs-clouds-doivent-etre-inquiets >.

LUNA, J., « D3.2 Risk-Based Decision Making Mechanisms For Cloud Service In The Public Sector», 31 Juillet 2017, en ligne : <https://www.cloudwatchhub.eu/sites/default/files/CloudWATCH2_Risk-based-decision-making-mechanisms-for-cloud-services.pdf>.

LEBLANC, J., « L'ordinateur quantique mettra l'internet K.O. » Québec science, 26 novembre 2016, en ligne : <https://www.quebecscience.qc.ca/technologie/lordinateur-quantique-mettra-linternet-k-o/>.

LE BOURLOUT, E., « Dropbox victime d'une faille de sécurité béante », *01net*, 21 juin 2011, en ligne : <http://www.01net.com/editorial/534667/dropbox-victime-d-une-faille-de-securite-beante/>.

LOUKIL, R., « Les cinq chiffres clés du cloud de Microsoft en 2018 », *L'UsineNouvelle*, (3 février 2019), en ligne : <https://www.usinenouvelle.com/article/les-quatre-chiffres-cles-du-cloud-de-microsoft-en-2018.N801215>.

LOVELLS, H., « Restoring Trust ? », *International Association of Privacy Professionnal*, 25 Juin 2015, en ligne : <https://iapp.org/news/a/usa-freedom-act-a-step-toward-restoring-trust/>.

MELL, P. et T. GRANCE, «The NIST definition of Cloud Computing», National Institute of Standards and Technology, September 2011, en ligne : <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

MICROSOFT CORPORATION, «Six Principles For International Agreements Governing Law- Enforcement Access To Data», en ligne : <https://blogs.microsoft.com/uploads/prod/sites/5/2018/09/SIX-PRINCIPLES-for-Law-enforcement-access-to-data.pdf>.

MICROSOFT CORPORATION, « Azure regions », 2019, en ligne : <https://azure.microsoft.com/en-ca/regions/>.

MICROSOFT CORPORATION, « Law enforcement requests », en ligne : <https://www.microsoft.com/en-us/corporate-responsibility/lerr>.

MICROSOFT CORPORATION, « Penetration Testing Rules of Engagement », 2019, en ligne : <https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1>.

MICROSOFT CORPORATION, « Rapports d'audit », en ligne : <https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide?command=Download&downloadType=Document&downloadId=e9db0154-b5c6-4570-9c63-c0c20b3519bc&docTab=4ce99610-c9c0-11e7-8c2c-f908a777fa4d_ISO_Reports>.

MICROSOFT CORPORATION, « Service Level Agreement Microsoft Azure », 2019, en ligne : <https://azure.microsoft.com/en-us/support/legal/sla/summary/>.

MICROSOFT CORPORATION, en ligne : <https://www.microsoft.com/en-ca/sites/datacentre/enterprise.aspx>.

MILLER, R. et J. CASTONGUAY, « rapport de projet sur : La gouvernance des grands projets d'infrastructure publique, La gestion des risques », Montréal, Mai 2006 en ligne : <https://cirano.qc.ca/files/publications/2006RP-17.pdf>.

MYERS, W. III, « Microsoft Azure Data Security (Data Cleansing and Leakage », *Microsoft Developer*, Septembre 2014, en ligne : <https://blogs.msdn.microsoft.com/walterm/2014/09/04/microsoft-azure-data-security-data-cleansing-and-leakage/>.

NATIONAL CONFERENCE OF STATE LEGISLATURE, «Security Breach Notification Laws» (29 septembre 2018), en ligne : <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE, « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », Éditions OCDE, 2019, en ligne : <http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelavieprive eetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm>.

RAN, G-B. N. DOWLIN, K. LAINE, K. LAUTER, M. NAEHRIG, et J. WERNSING. « Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. » In International Conference on Machine Learning, 2016, en ligne : <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/04/CryptonetsTechReport.pdf>.

REIMER, J., « Total Share: 30 Years of Personal Computer Market Share Figures », (15 décembre 2005) *Ars Technica*, en ligne : <https://arstechnica.com/features/2005/12/total-share/>.

SANGHAVI, P., « why do we use a cloud as the shape to represent things like SkyDrive, iCloud, etc.? », *Quora*, 1er Février 2015, en ligne : <https://www.quora.com/Why-do-we-use-a-cloud-as-the-shape-to-represent-things-like-SkyDrive-iCloud-etc>.

SHERWEB | Blog, « Microsoft Azure's Canadian Cloud Servers: A True Canadian Cloud? », 10 juin 2016, en ligne : <http://www.sherweb.com/blog/azure-canadian-cloud/>.

SIMORJAY, F., « Shared Responsibilities for Cloud Computing », *Microsoft TechNet*, Avril 2017, en ligne : <http://aka.ms/sharedresponsibility>.

SMITH, B., « A call for principle-based international agreements to govern law enforcement access to data », *Microsoft On the Issues*, blog, 11 Septembre 2018, en ligne : <https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/>.

SRIVASTAVA, S., « Maintenance for virtual machines in Azure », Microsoft Azure, Décembre 2018, en ligne : <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/planned-maintenance>, (consulté le 28 avril 2019).

SULLIVAN, D. « a brief history of decentralized computing », (Août 2018) *Samsung NEXT*, en ligne : <https://samsungnext.com/whats-next/a-brief-history-of-decentralized-computing/>.

TARABAY, J. « Australian Government Passes Contentious Encryption Law», *NY Times*, (Décembre 2018), en ligne : <https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html>.

TRUDEL P. (entrevue de M. BEAUMONT), « Les données personnelles: enjeu majeur. » FM 98.5 *Puisqu'il faut se lever*, 8 Janvier 2019., en ligne : <https://www.985fm.ca/extraits-audios/opinions/180324/entrevue-me-pierre-trudel>.

UNIVERSITÉ DE MONTRÉAL, Bibliothèque « Gestion des données de recherche », en ligne : <https://bib.umontreal.ca/gerer-diffuser/gestion-donnees-recherche>.

UNIVERSITÉ DE MONTRÉAL, Secrétariat général, « Règlements, directives, politiques et procédures », en ligne : < https://secretariatgeneral.umontreal.ca/documents-officiels/reglements-et-politiques/>.

UNIVERSITÉ LAVAL, « Directive relative à la gestion des renseignements personnels et du matériel Biologique recueillis dans le cadre de projets de recherche impliquant des sujets humains », 20 Avril 2005, en ligne : <https://www.ulaval.ca/fileadmin/ulaval_ca/Images/recherche/Documents/Politiques/Directives_bd_renseignement_personnels_CA.pdf>.

UNIVERTISÉ D'OTTAWA, « Règlement 117 – Classification et manutention de l'information », en ligne : <https://www.uottawa.ca/administration-et-gouvernance/reglement-117-classification-manutention-information>.

UNIVERSITY OF CALIFORNIA, BERKELEY, «Data classification standard», 16 juillet 2012 (Administrative revision: April 22, 2013) en ligne : <https://security.berkeley.edu/data-classification-standard>.

VERMEYS, N. W., Table ronde lors de l'émission « Faut pas croire tout ce qu'on dit », au cours de l'épisode intitulé : « Le Québec entend confier au privé les données personnelles qu'il détient sur ces citoyens » 9 février 2019.

# Annexe 1 : Analyse de Risque

1. Les risques organisationnels :

**R.1 : Fermeture ou changement du service infonuagiques**

Des litiges avec le fournisseur infonuagique ou la non-rentabilité des services peuvent entrainer la cessation des services infonuagique[610], sans oublier les achats[611] ou les engloutissements par la compétition ayant des pratiques différentes en ce qui a trait à la sécurité de l'information.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Très faible | Non applicable |
| Gravité | Très élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Confidentialité | |
| Niveau du risque | Moyen | |

**R.2 : Vendor-Lock-In**

Il y a peu de moyens de garantir une transférabilité des services infonuagique. Dans l'IaaS, puisque l'infrastructure est contrôlée presque en totalité par l'université cliente du service, le « lock-in » sera habituellement au niveau de l'hyperviseur[612].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Élevé | Presque inexistante |
| Gravité | Moyen | Presque inexistante |
| Obligation de sécurité affectée | Disponibilité, Confidentialité | |
| Niveau du risque | Moyen | |

[610] Id,. préc., note 206;
[611] *Oracle Canada* c. *Centre intégré universitaire de santé et de services sociaux du Centre-Sud-de-l'Île de Montréal*, 2018 QCCA 10.
[612] OQLF., préc., note 10, « hyperviseur » : « Logiciel de virtualisation qui supervise l'allocation dynamique des ressources à chacune des machines virtuelles qu'il contribue à créer et à administrer. ».

**R.3 : Perte de gouvernance (Continuité des activités[613] et résilience)**

En utilisant l'IaaS, le client cède nécessairement le contrôle de ses données au prestataire de service infonuagique, ce qui a pour conséquence de lui faire perdre la capacité de déployer les mesures organisationnelles et techniques nécessaires pour garantir la disponibilité, l'intégrité et la confidentialité de ces données. Certains auteurs[614] avancent que la perte de gouvernance sera moins importante lorsqu'on impartira en modèle IaaS puisque presque l'intégralité de la responsabilité de l'infrastructure demeure aux mains du client[615]. De notre point de vue[616], c'est plutôt l'effet inverse qui se produit. En transférant l'infrastructure informatique en partie ou en totalité sur des systèmes gérés par des prestataires de services infonuagiques, bien que le contrôle soit sous la responsabilité du client, les conditions d'utilisation des services pourront notamment nous empêcher d'effectuer des balayages de port[617], l'évaluation des vulnérabilités ou encore des tests d'intrusions[618], qui entraîneront à eux seuls de grands risques pour la sécurité.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Élevé | Presque inexistante |
| Gravité | Élevé[619] | Presque inexistante |
| Obligation de sécurité affectée | Disponibilité, Confidentialité | |

[613] OQLF., préc., note 10, « plan de continuité des activités » : « 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 ».

[614] *Id*., préc., note 372.

[615] Dans un système IaaS, il est question de responsabilité partagé : par exemples dans le cas du IaaS, Microsoft se dit être responsable de la sécurité des lieux physiques ainsi que partiellement du bon fonctionnement des machines virtuelles et du réseau informatiques, tonnons aussi que « *This responsibility includes the configuration of the permissions and network access controls required to ensure that networks can communicate correctly and that devices are able to attach or mount the correct storage devices.* » voir notamment Frank SIMORJAY, « Shared Responsibilities for Cloud Computing », *Microsoft TechNet*, Avril 2017, en ligne : <http://aka.ms/sharedresponsibility>, (consulté le 28 avril 2019).

[616] Nous partageons le point de vue de l'ENISA ainsi que celui du CSA.

[617] OQLF., préc., note 10, « Balayage de port » : « *Technique consistant à balayer automatiquement, à l'aide d'un programme approprié, une série d'adresses IP spécifiques, afin de trouver et d'examiner les ports ouverts sur chaque ordinateur en réseau, puis d'exploiter ces failles de sécurité en vue d'une intrusion.* ».

[618] OQLF., préc., note 10, « Test d'intrusion » : « *Test au cours duquel un spécialiste tente de pénétrer dans un réseau de systèmes informatiques dans les mêmes conditions qu'un intrus éventuel, afin de vérifier l'efficacité des dispositifs de sécurité mis en place et d'éliminer les failles décelées grâce à cette opération.* ».

[619] Plus le niveau d'impartition est important, plus les incidences sur la gouvernance le seront, IaaS, très importante, PaaS, moyennement important, SaaS moins important.

| | |
|---|---|
| Niveau du risque | Élevé |

**R.4 : Défaillance d'un des acteurs liés au service infonuagique**

Un fournisseur de service infonuagique peut sous-traiter certaines tâches spécialisées à des tiers. Dans une telle situation, le niveau de sécurité global aura une corrélation directe avec les niveaux de sécurité de chacun des liens et du niveau de dépendance du fournisseur d'infonuagique sur le ou les tiers.[620]

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Élevé | Non applicable |
| Gravité | Élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |

**R.5 : Perte de conformité**

L'investissement de l'organisation pour obtenir des certifications pour répondre à certaines exigences réglementaires pourra être mis en péril par une migration vers l'infonuagique dans le cas où le prestataire de service ne peut fournir la preuve de sa propre conformité, ou lorsqu'il ne permet pas la vérification (audit) par le client ou un tiers.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyenne | Non applicable |
| Gravité | Faible | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Faible | |

[620] *Loi sur l'accès*, art. 70.1.

**R.6 : Perte de disponibilité due aux activités des colocataires des services infonuagiques.**

Le partage des ressources signifie que les activités malveillantes effectuées par un locataire pourraient avoir des répercussions sur les services offerts à une autre institution utilisatrice[621].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Faible | Non applicable |
| Gravité | Élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Confidentialité | |
| Niveau du risque | Moyen | |

## 2. Les risques techniques :

**R.7 Panne matérielle liée au réseau**

Les interruptions, la congestion[622], les mauvaises connexions, l'utilisation non optimale et la modification du trafic réseau sont des risques présents lorsqu'on utilise une infrastructure reposant sur un service hébergé à l'extérieur des établissements d'enseignement. Ces risques peuvent être grandement réduits puisque certains fournisseurs offrent désormais des connexions privées[623] entre leurs centres de données et l'infrastructure qui se trouve sur les sites des clients, ce qui aura pour effet de garantir une certaine connectivité aux services infonuagique.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Non applicable |
| Gravité | Élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Intégrité | |
| Niveau du risque | Moyen | |

[621] L'ENISA mentionne entre autres qu'une mauvaise utilisation par un locataire pourrait entraîner le blocage d'une gamme d'adresse IP, ou la confiscation des ressources par une autorité compétente.
[622] Certains fournisseurs d'infonuagique peuvent effectuer de la limitation au gros utilisateur de bande passante.
[623] Notons par exemple ExpressRoute de Microsoft, CloudInterconnect de Google & AWS Direct Connect.

**R.8 Épuisement des ressources (sous provisionnement)**

L'infonuagique est un service à la demande. Une mauvaise prévision, ou une modélisation inexacte du niveau d'utilisation des ressources pourraient entrainer une indisponibilité des ressources suite à une saturation de celles-ci. L'erreur peut être commise par le fournisseur, mais également par le gestionnaire de l'université responsable de l'infrastructure. Une instance peut également s'accroitre automatiquement en puisant parmi des crédits lors de hausses soudaines du niveau des services demandés. Des fonds minimums et un contrôle des coûts doivent être alors observés pour assurer une telle croissance des services sans interruption.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Non applicable |
| Gravité | Élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité | |
| Niveau du risque | Moyen | |

**R.9 Échec d'isolement**

Le regroupement des ressources et l'utilisation de « tenant multiple »[624] sont des caractéristiques fondamentales de l'infonuagique, comme nous l'avons soulevé précédemment. Par contre, si elles sont incorrectement employées, elles peuvent échouer la fragmentation d'éléments clés tels que le stockage, la mémoire ou encore le routage et par le fait même occasionner des risques ou des infections entre les « locataires » des services d'IaaS.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus faible que l'IaaS |
| Gravité | Très élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |

[624] T. ERL, Z. MAHMOOD, R. PUTTINI, préc., note 29, p. 106-107.

**R.10 Abus malveillants de provenance interne – abu de privilèges**

Les activités malveillantes d'un employé du service infonuagique pourraient potentiellement avoir de lourde conséquence sur la disponibilité, l'intégrité ou la confidentialité des données propres à l'infrastructure déportée de l'université. Des occasions comme celles-ci peuvent se produire malgré que les infrastructures sous forme de service soient habituellement soumises à une surveillance accrue comparativement à certaines infrastructures localement administrées. Comme les IaaS regroupent habituellement un large spectre de client, les employés du fournisseur de service n'ont pas d'attache avec les nombreuses compagnies et peuvent être moins sensibles aux problèmes liés aux obligations de sécurité.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus élevé que l'IaaS |
| Gravité | Élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

**R.11 Piratage de compte ou de services (y compris l'interface de gestion)**

Les interfaces de gestion des clients infonuagique sont accessibles depuis l'Internet. Ils présentent donc un risque accru, surtout lorsqu'on y ajoute les vulnérabilités d'accès distant et des navigateurs web[625].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus faible que l'IaaS |
| Gravité | Très élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |

[625] OQLF., préc., note 10, « Navigateur web » : « Logiciel client capable d'exploiter les ressources hypertextes et hypermédias du Web ainsi que les ressources d'Internet dans son ensemble, qui permet donc la recherche d'information et l'accès à cette information. ».

**R.12 Déni de services distribués (DDoS)**

Le DDoS[626] est une attaque informatique par saturation des serveurs d'une société, elle permet de paralyser l'accès aux internautes aux services visés. L'IaaS, comme tous les modèles infonuagiques ne sont pas à l'abri de ces attaques[627].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Client : Moyen | Plus faible que l'IaaS |
| | Fournisseur : Faible | Non applicable |
| Gravité | Client : Élevé | Plus élevé que l'IaaS |
| | Fournisseur : Très élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Intégrité | |
| Niveau du risque | Moyen | |

[626] OQLF., préc., note 10, « Distributed Denial of Service » : « Attaque informatique qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes. ».

[627] Voir à cet effet, Jennifer A. CHANDLER, «Improving Software Security: A Discussion of Liability for Unreasonably Insecure Software». SECURING PRIVACY IN THE INTERNET AGE, *Stanford University Press*, 2006. en ligne : <https://ssrn.com/abstract=610041>; Jennifer A. CHANDLER « Security in Cyberspace: Combatting Distributed Denial of Service Attacks», 2004, p231-261

**R.13 Vulnérabilités logiciels**

Tous les logiciels sont susceptibles d'être affectés par des vulnérabilités qui peuvent causer une défaillance d'un des systèmes ou permettre une intrusion. Les infrastructures infonuagiques reposent sur des technologies logicielles qui sont également sujettes à être affecté par ces vulnérabilités. Chacune des couches y est prédisposée, de l'hyperviseur aux interfaces de gestion. De plus, certaines rustines peuvent créer des problèmes d'interopérabilité avec les outils déjà en place. Lorsque ces corrections sont apportées, les fournisseurs de service n'informent pas nécessairement les clients des changements effectués[628].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus faible que l'IaaS |
| Gravité | Élevé | Très élevé |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

**R.14 La perte ou vol de sauvegarde**

La pérennité des documents est une notion imprégnée à l'intégrité des données, mais la perte ou le vol d'une sauvegarde peuvent aussi avoir une répercussion sur la disponibilité (en cas de besoin de restauration) ainsi que sur le schème de la confidentialité, dans l'optique où un vol est perpétré dans le but de dérober de l'information.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Faible | Plus faible que l'IaaS |
| Gravité | Élevé | Élevé |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

[628] *« The Cloud Service Provider will operate and secure the host services, such as the operating systems of the service. »* : Si par exemple, une faille de sécurité sur un OS pouvait rendre vulnérable l'infrastructure, Microsoft pourrait appliquer la rustine elle-même, voir à cet effet: *Shared Responsibilities for Cloud Computing* en ligne : <http://aka.ms/sharedresponsibility>.

**R.15 La perte, la divulgation ou la corruption des clés de chiffrement**

La perte des clés de chiffrement (SSL, chiffrement des fichiers, clés privées du client) ou des mots de passe constitue un risque important pour les Infrastructures sous forme de service[629].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Faible | Non applicable |
| Gravité | Élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

**R.16 Escalade des privilèges**

Une élévation des privilèges est, en informatique, un mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement[630].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Faible | Plus faible que l'IaaS |
| Gravité | Élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

[629] Id,. préc., note 208.
[630] Voir à ce sujet David BASIN, Patrick SCHALLER, Michael SCHLÄPFER, *Applied Information Security- A Hands-on Approach,* Springer, Berlin, Heidelberg, 2011, page 88.

**R.17 Les attaques d'ingénierie sociale**

Les emprunts d'identité[631], l'usurpation[632], ou les tentatives de flouer la naïveté de certains utilisateurs, sont une des attaques rependues[633]. Les usagers des IaaS ne sont pas à l'abri de ces phénomènes. Par ailleurs, l'inexpérience ou l'impéritie de certains devant l'infonuagique peut accentuer la possibilité d'être floué.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Comparable |
| Gravité | Élevé | Comparable |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

**R.18 Interception des données en transit**

L'infrastructure sous forme de service repose bien entendu sur une architecture distribuée. Cette notion implique beaucoup de données en transit en provenance, ainsi qu'en direction des universités.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus faible que l'IaaS |
| Gravité | Élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

[631] Le Code Criminel définit le Vol d'identité par : « *402.2 (1) Commet une infraction quiconque obtient ou a en sa possession des renseignements identificateurs sur une autre personne dans l'intention de ls utiliser pour commettre un acte criminel dont l'un des éléments constitutifs est la fraude, la supercherie ou le mensonge ou ne se souciant pas de savoir si tel sera le cas.* »

[632] Article 56 C.c.Q.

[633] Voir par exemple *Laliberté c. Transit Éditeur inc*., 2009 QCCS 6177 (CanLII)

**R.19 Suppression non sécuritaire ou inefficace des données**

Lorsque les ressources utilisées sont réduites, le matériel physique est réassigné, les données peuvent alors demeurer disponibles au-delà de la durée de vie spécifiée dans la stratégie de sécurité. Ce concept est défini clairement dans la notion d'intégrité de la triade.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus faible que l'IaaS |
| Gravité | Très élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |

**R.20 La perte, la compromission ou l'inexistence des « journaux »[634] d'opération et de sécurité**

Afin d'apprécier l'intégrité d'une donnée, il est essentiel de pouvoir suivre les changements au fil de son cycle de vie[635]. Pour ce faire, l'enregistrement événementiel de son état doit être accessible par les utilisateurs de IaaS.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Faible | Faible |
| Gravité | Moyen | Faible |
| Obligation de sécurité affectée | Intégrité | |
| Niveau du risque | Moyen | |

[634] OQLF., préc., note 10, « journaux » : « Fichier contenant les données historiques de l'exploitation d'un système sur une période donnée qui est constitué à des fins de sécurité informatique. ».
[635] LCCJTI, art. 6.

**R.21 Catastrophes naturelles**

Basés sur la situation géographique et le climat, les centres de données peuvent être exposés à des catastrophes naturelles telles que la foudre, les tempêtes et les tremblements de terre, qui peuvent en affecter les services infonuagiques. Compte tenu de la ségrégation des centres de données, la probabilité de répercussion est considérablement plus faible que si une infrastructure conventionnelle est employée.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Très faible | Plus élevé que l'IaaS |
| Gravité | Élevé | Élevé |
| Obligation de sécurité affectée | Disponibilité | |
| Niveau du risque | Moyen | |

**R.22 Accès non autorisé/vol d'équipement (accès physiques aux installations)**

Les accès non autorisés aux installations physiques ne sont jamais souhaités. Néanmoins, les contrôles de sécurité sont susceptibles d'être plus rigoureux dans un vaste centre de données.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Très faible | Comparable |
| Gravité | Élevé | Plus élevé que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Moyen | |

**R.23 Erreur humaine (interne ou externe)**

L'application inadéquate des procédures de base de sécurité ou des bévues accidentelles d'administrateur d'infrastructure peuvent occasionner des risques importants.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Élevé | Comparable |
| Gravité | Élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |

## 3. Les risques légaux

**R.25 Confiscation d'équipement par les autorités légales pour criminalistique.**

Dans le cas d'une privation de matériel par des organismes d'application de la loi, la centralisation des infrastructures ainsi que le partage de ressources informatiques signifient un risque accru à la disponibilité des données.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Élevé | Plus faible que l'IaaS |
| Gravité | Moyen | Comparable |
| Obligation de sécurité affectée | Disponibilité | |
| Niveau du risque | Moyen | |

**R.26 Risque de changement de juridiction**[636]

Les données du client peuvent être détenues dans plusieurs juridictions dans lesquels différentes lois sont sujettes à s'appliquer. Notons également que *« lorsque les données ne sont pas localisées, la juridiction ayant compétence pour traiter un litige éventuel sera par ailleurs difficile à déterminer.* »[637].

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Très élevé | Non applicable |
| Gravité | Élevé | Non applicable |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |

[636] *Loi sur l'accès*, art. 70.1.
[637] N. W. VERMEYS, J. M. GAUTHIER et S. MIZRAHI, préc., note. 54, p. 141.

**R.27 Risque lié aux licences**

Les conditions d'utilisations de certaines licences peuvent parfois restreindre l'emplacement géographique de la disponibilité, limiter l'utilisation à distance de certains outils, ou même limiter l'utilisation par certaines nationalités étrangères. Ces conditions devront faire l'objet de vérification auprès du contentieux de l'université pour assurer leurs conformités. Les risques d'une anomalie à l'utilisation sont accentués lorsque celle-ci est faite à l'extérieur des universités.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Moyen | Plus faible que l'IaaS |
| Gravité | Moyen | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité | |
| Niveau du risque | Moyen | |

**R.28 Risque d'obligation de sécurité**

Le dernier risque, mais non le moindre, est sans aucun doute les risques liés à l'obligation de sécurité elle-même. Nous avons soulevé des risques pouvant possiblement affecter l'un ou l'autre des éléments de la triade de la sécurité informationnelle. Par contre, ces éléments sont accompagnés de lois et de règlements encadrant leurs applications. Ils seront, bien entendu, d'une importance capitale et ne pas suivre leurs lignes directrices pourra sans aucun doute avoir des répercussions judiciaires importantes, qui posent elles-mêmes des risques pour les utilisateurs d'IaaS.

| | IaaS | Infrastructure conventionnelle |
|---|---|---|
| Probabilité | Élevé | Plus faible que l'IaaS |
| Gravité | Élevé | Plus faible que l'IaaS |
| Obligation de sécurité affectée | Disponibilité, Intégrité, Confidentialité | |
| Niveau du risque | Élevé | |