Basma Makhlouf Shabou et Valérie Léveillé. Records in the Cloud. In : Actes du 43e Congrès de l'Association des archivistes du Québec (AAQ), Montréal, 28-30 mai 2014.

Records in the Cloud

Résumé

Initié en 2012 par l'Université de Colombie-Britannique(UBC) sous la direction de la Professeure Luciana Duranti de la *School of Library, Archival and Information Studies* (SLAIS) et soutenu par le Conseil de recherches en sciences humaines du Canada (CRSH), le projet Records in the Cloud (RiC, http://www.recordsinthecloud.org) vise à identifier et à analyser en profondeur les questions techniques, opérationnelles, juridiques et économiques relatives au traitement et à la conservation externalisés moyennant des options Cloud. Basé sur une approche qualitative, ce projet réunit un groupe interdisciplinaire et international de chercheurs nord-américains et européens. Il ambitionne de développer les politiques, les directives, les outils et les dispositifs répondant aux besoins des utilisateurs et des fournisseurs des services Cloud. Au terme de cette recherche, un éclairage pertinent sur les avantages et les risques qui caractérisent les pratiques de la gestion des documents via les solutions Cloud sera présenté. Sur le plan méthodologique, en plus de l'analyse exhaustive de la littérature scientifique et professionnelle, un questionnaire web auprès de 300 utilisateurs Cloud et des entretiens semi-structurés d'un échantillon significatif de fournisseurs Cloud sont envisagés.

Nous présenterons dans cet article deux sections principales. La première sera réservée à la présentation des grandes lignes du projet RiC: sa problématique, ses objectifs et ses questions de recherche en détaillant la méthodologie préconisée pour ses quatre années de réalisation. Nous y préciserons, également, les différentes étapes réalisées et rappellerons les étapes prévues dans le cadre de cette recherche. La deuxième section présentera les résultats préliminaires de cette recherche.

INTRODUCTION

Le «Cloud» est un environnement virtuel et une infrastructure informatique qui comprend toutes les aptitudes d'un système informatique qui sert à remplacer l'infrastructure physique et interne — c'est-à-dire les logiciels, l'équipement de réseau, etc. – qu'aurait autrement stockée une compagnie. La gestion de ce nouvel environnement est fournie par un ou plusieurs tiers, les fournisseurs externes, dont le service est caractérisé par cinq aspects essentiels: (1) des ressources en libre-service et adaptation automatique à la demande, c'est-à-dire aux besoins du consommateur; (2) l'ouverture, c'est-à-dire que les services Cloud sont mis à disposition sur internet et l'utilisateur peut y accéder à n'importe quel instant via n'importe quel appareil (ordinateur, tablette, etc.); (3) la mutualisation, c'est-à-dire que le Cloud peut être un environnement à multi tenant, où des ressources hétérogènes (matériel, logiciel, trafic réseau, etc.) sont partagées entre plusieurs consommateurs à la fois; (4) l'élasticité, qui permet d'adapter automatiquement les ressources du Cloud d'après les demandes et les besoins du consommateur; et (5) des services mesurés où les paiements sont accessibles via un réseau informatique, par exemple l'internet.

Les options Cloud peuvent être rationalisées, c'est-à-dire que la quantité des services (ex.: stockage, bande passante, traitement, etc.) consommée dans le Cloud est mesurée, à des fins de contrôle, de reportage, d'adaptation des moyens techniques, et de facturation. Ces caractéristiques sont censées aider l'utilisateur à gérer, de manière économique, appropriée et rationnelle, ses besoins en matière de traitement et de stockage des données.

Généralement, nous pouvons reconnaître trois types de services principaux du Cloud: *Software as a Service* ou logiciel en tant que service (SaaS), *Platform as a Service* ou plate-forme en tant que service (PaaS), et *Infrastructure as a Service* ou infrastructure en tant que service (IaaS). Le choix des utilisateurs n'est pas forcément restreint à un seul type de Cloud. Plusieurs formules et combinaisons sont envisageables et définissables selon l'importance et la nature des besoins des utilisateurs. Il importe de noter également qu'en plus de ces trois types de Cloud de base, il existe d'autres types de services Cloud comme celui qui a été considéré par la Stratégie suisse d'informatique en nuage (2012-2020)[1], qui fournit le processus métier comme service (ex.: *Business Process as a Service* (BPaaS)). L'IaaS offre à l'utilisateur un plus haut niveau de contrôle en lui offrant accès au système virtuel même, tandis que le SaaS met seulement des applications du Cloud à la disposition de l'utilisateur (ex. Gmail, iCloud, Google Docs, etc.), qui fait en sorte qu'il exerce peu de contrôle sur le développement et les paramètres de l'application.

De plus, il existe quatre différents modèles de déploiement du Cloud: le Cloud public dont le service est partagé entre un large public, le Cloud communautaire où plusieurs utilisateurs ayant des préoccupations et des intérêts communs profitants des mêmes services en partageant un même Cloud, le Cloud privé qui est réservé pour un seul et unique utilisateur, et le Cloud hybride qui comprend des caractéristiques des Cloud public et privé. Chaque modèle augmente ou diminue le niveau de sécurité de ses données, correspondant ainsi à une augmentation ou à une diminution du prix que paiera l'utilisateur.

La qualité souhaitée dans la gestion des données dans le Cloud et le lien de confiance qui peut être développé entre l'utilisateur consommateur et le fournisseur à cet égard posent en soi une problématique. Quelle est la réalité en ce qui concerne la sécurité des données dans le Cloud? Quelles sont les attentes envers le fournisseur du Cloud pour ce qui en est de la sécurité des données? Envers le consommateur? Et peut-on entièrement faire confiance aux fournisseurs qui s'occupent de la protection ultime des données dans le Cloud? Ces questions concernent non seulement la gestion des données, mais aussi la préservation, à long terme, de ces données dans le Cloud.

Nous présenterons dans cet article, les grandes lignes du projet RiC. Pour ce faire, la méthodologie sera exposée et les principaux résultats seront décrits pour ensuite finir avec un aperçu de la suite des étapes prévues jusqu'à la fin de cette recherche.

[1]Unité de pilotage informatique de la Confédération UPIC. 2013. Stratégie suisse d'informatique en nuage. Confédération suisse. [site web]. http://www.isb.admin.ch/themen/strategien/01603/index.html?lang=fr.

Présentation du projet RiC

Records *in the Cloud* (RiC) est un projet de recherche collaboratif, financé par le Conseil de recherches en sciences humaines (CRSH), qui réunit la *School of Library, Archival and Information Studies* (SLAIS), *Faculty of Law*, and the *Sauder School of Business* de l'Université de la Colombie-Britannique (UBC); l'École de l'information de l'Université de Washington; l'École de l'information et de bibliothéconomie de Chapel Hill en Caroline du Nord; le Département d'Informatique et des médias de l'université Mid-Sweden; la Haute école de gestion de Genève (HEG); et le *Cloud Security Alliance* (CSA).

La réalisation de cette recherche, menant des initiatives interdisciplinaires d'envergure internationale, est prévue sur une période de 4 ans. Ses objectifs sont les suivants:

- Identifier et examiner les questions de gestion opérationnelles, juridiques, et techniques qui concernent la gestion et le stockage des données dans le Cloud;

- Déterminer quelles pratiques et politiques un fournisseur de Cloud devrait avoir en place afin d'être capable de faire la mise en œuvre complète du système de gestion des données et/ou des archives de l'organisation qui choisit de confier son information à ce fournisseur. Cet objectif consiste à préciser les exigences à édifier pour qu'un fournisseur soit en mesure de répondre aux besoins de l'utilisateur, ainsi que de reconnaître, identifier, analyser et résoudre n'importe quel incident qui risque de se produire;

- Développer des directives qui peuvent guider les utilisateurs courants et potentiels à évaluer adéquatement les risques et les avantages de placer leurs données dans le Cloud, à négocier des accords de service (*Service Level Agreement*), à reconnaître des certificats et/ou des attestations de service, et à bien guider l'intégration de leur programme de gestion des données et/ou des archives avec celui du nouvel environnement Cloud.

Méthodologie

Comme précisé, cette recherche vise essentiellement trois volets: d'abord (1) identifier et examiner, en détail, les problèmes opérationnels, légaux et techniques qui se posent avec le stockage et la gestion des documents dans le Cloud; ensuite (2) formuler des politiques et procédures que les fournisseurs devraient suivre afin de démontrer, à ceux qui leur confient leurs documents, qu'ils sont aptes de gérer leurs données d'une manière qui reflète la façon dont on gère l'information ou les archives au sein de l'organisation même, de répondre adéquatement aux besoins de l'organisation, et de discerner, d'identifier, d'analyser et de répondre aux problèmes qui se posent; et enfin (3) développer des lignes directrices pour les consommateurs cherchant à évaluer les risques et les bénéfices de se positionner envers l'externalisation du stockage de leurs informations et/ou archives vers un Cloud, de négocier des dispositions contractuelles, des certifications et/ou des attestations, et d'assurer l'intégration

des pratiques et politiques surveillant la gouvernance de l'information au sein de l'organisation avec le nouvel environnement dans lequel se retrouvent leurs données.

Pour ce faire, cette recherche préconise une approche qualitative qui s'appuie sur des connaissances multidisciplinaires considérant les principes et fondamentaux de la théorie archivistique contemporaine, de la diplomatique, ainsi que ceux de l'informatique. La collecte des données se fera par quatre modes: (1) une analyse documentaire de la littérature portant principalement sur la gestion de l'information dans le Cloud; (2) une recherche de législations, de règlementation, de jurisprudence, et de standards relatifs à la gestion et à l'entreposage des données dans le Cloud; (3) la réalisation d'un questionnaire auprès des utilisateurs du Cloud; et (4) la réalisation d'entrevues semi-structurées sur les services offerts par divers fournisseurs du Cloud, ainsi que des technologies qu'ils utilisent. Cette collecte de données sera suivie par une analyse exhaustive, qui comprend la transcription des entrevues diverses, la comparaison entre l'information transmise par les fournisseurs du Cloud avec celle obtenue par le biais des utilisateurs, et le dépouillement des données recueillies auprès des utilisateurs.

Jusqu'à présent, le résumé de l'ensemble a été transmis sous forme de bilan, d'essais, de rapports, et de communications diverses (ex.: présentations données lors des colloques, conférences, etc.): par exemple, un rapport sur les résultats du questionnaire des utilisateurs, ou *User Survey Report* (Pan, Rowe & Barlaoura, 2013), et un texte traitant des effets de la directive sur la protection des données de l'Union européenne sur le Cloud intitulé «*Cloud computing and Risk: A look at the EU and the application of the Data Protection Directive to cloud computing* » (Ostrzenski, 2013). Le texte qui suit approfondira davantage les résultats des quatre modes énumérés ci-dessus.

Présentation des résultats préliminaires

Les résultats de la présente recherche sont nombreux et variés. Dans ce chapitre, nous proposons un aperçu des principaux résultats préliminaires obtenus à la suite de l'avancement des différents modes de collecte des données réalisés jusqu'ici, à savoir la revue de la littérature, les entrevues semi-structurées et le questionnaire en ligne.

Analyse de la littérature

Une des premières stratégies de recherche pour la collecte des données s'est réalisée par le biais de l'analyse de la littérature. En premier lieu, il eut une analyse générale de la documentation et des textes qui se rapportaient à l'entretien des documents et des données dans le Cloud. Ceci a compris la revue d'articles de journaux, de livres, de blogues, de sites web et de rapports divers, etc. traitant de la création, la gestion, l'utilisation, l'entreposage, la conservation à long terme et l'accès continu à l'information et aux documents entreposés dans le Cloud. Bien que le mouvement vers le Cloud soit un concept relativement nouveau (la majorité des textes publiés datant entre 2006 et 2013), l'étendue de la littérature se rapportant au Cloud est vaste et traite de sujets divers. D'abord, on remarque un inventaire de textes se rapportant à l'architecture du Cloud (Wang, He & Wang, 2012), y compris les différents types d'acteurs dans le Cloud (ex.: consommateur, fournisseur, vérificateur, courtier, transporteur, etc.), les différents modèles de service du Cloud (ex: logiciel en tant que service ou SaaS;

Plateforme en tant que service ou PaaS; infrastructure en tant que service ou IaaS), ou les différents modèles de déploiement (ex.: le Cloud privé; le Cloud public; le Cloud communautaire; le Cloud hybride). La sécurité des données (par exemple le contrôle à l'accès aux données, la communication sécurisée, le chiffrement (*encryption*)), la gestion de l'identité, les pistes d'audit et l'établissement de la provenance des documents dans le Cloud (Mohammed, 2011; Gold, 2012; Julisch et Hall, 2010; Muthulakshmi et al., 2013; Shabeeb et al., 2012; Shaikh et Sasikumar, 2012; Sing et Shrivastava, 2012; Subashini et Kavitha, 2010; Zissis et Lekkas, 2011), ainsi que la vie privée et la protection des données personnelles (Katzan, 2010; Kesan et al., 2013) sont aussi des thèmes récurrents dans le survol de la littérature explorée pour cette étude. La conservation des données dans le Cloud est aussi un sujet souvent abordé (Ashkoi et al., 2011); les problèmes qui sont posés par le Cloud quant à la conservation à long terme des documents d'archives électroniques sont des sujets qui préoccupent les archivistes et les gestionnaires d'aujourd'hui. Plus récemment, on voit paraître plusieurs textes traitant des questions d'admissibilité juridique, de recevabilité des documents et des données entreposées dans le Cloud, et les enquêtes juridico-informatiques (*digital forensics*) (Araiza, 2011; Gray, 2013; Grounds et Cheesbro, 2013; Chung et al., 2012; Li et al., 2013). Les questions portant sur la gouvernance de l'information, l'intégrité des données et la gestion des données dans le Cloud (Cunningham, 2012; Stuart et Bromage, 2010) sont souvent abordées de manière générale; plusieurs de ceux-ci ont même été des sujets importants de rapports, de lignes directrices ou de *white paper* qui sont maintenant consultés en tant que sources importantes pour la mise en place du Cloud (Autonomy, 2012; Badger et al., 2012; Gauthersburg et al., 2009; Breuning et Treacy, 2009; Dubourg, 2014; Unité de Stratégie Informatique de la Confédération, 2011; Gellman, 2009; Hogan et al., 2011; Jansen et Grance, 2011). De plus et faisant le lien encore plus précisément aux objectifs de l'initiative RiC, il eut plusieurs publications se rapportant à la création d'un climat de confiance dans Cloud, un sujet qui n'est pas nécessairement aussi récent qu'on l'aurait deviné (Ahamed et Sharmin, 2008; Basu et Callaghan, 2005; Fan et al., 2012), mais qui n'a toujours pas été résolu.

Il eut également une analyse de documentation et de textes juridiques et normatifs (loi, règlements, jurisprudence, et standards) relatifs à l'entreposage des données dans le Cloud. La nature «sans frontière» du Cloud – c'est-à-dire que mettre nos données dans le Cloud prétend que nous ne savons pas exactement où se retrouvent celles-ci – fait en sorte que la question de la place du Cloud dans la loi et les législations n'a pas le choix que d'être étudiée sur l'échelle internationale.

L'harmonisation des lois et des règles internationales

La question de l'harmonisation des lois a été explorée en détail lors de la recherche sur les lois et les législations. Le processus qu'entend l'harmonisation des lois comprend quatre composantes: les instruments, les acteurs, les intérêts et les inquiétudes, et les théories sous-jacentes. D'abord, il existe plusieurs instruments (ex.: *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*; *The EU Data Directive*; *The Budapest Convention on Cybercrim*e; *The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*; et *The APEC Privacy Framework*) qui servent d'exemples de lois dites harmonisées. Souvent, l'harmonisation des lois entend la participation de certains acteurs au niveau de la rédaction d'une loi ou d'une convention telle quelle; cette collaboration peut ainsi avoir un effet considérable sur le succès de l'outil ou du produit final et de son adoption. Ces acteurs s'intéressent donc le plus au résultat et à l'impact que ces instruments auront sur la communauté pour laquelle ils ont été rédigés. Bien que l'Union Européenne, la Convention de l'Europe, l'OECD et l'APEC se comptent parmi les acteurs principaux, plusieurs

gouvernements, d'autres organisations commerciales et d'autres entreprises ont eux aussi souvent à jouer un rôle non seulement dans le processus de rédaction de ces conventions. Pouvons-nous supposer que ceci est vrai aussi pour l'adoption et l'implémentation d'autres types d'instruments? Si oui, il est important d'identifier, dès le début, les acteurs principaux qui joueront un rôle clé dans l'adoption de l'instrument une fois complété.

Suite à l'identification d'acteurs principaux, il suffit aussi de développer l'initiative de manière à ce qu'elle soit compréhensible et capable de se traduire à plusieurs niveaux, dans divers domaines, peu importe le pays ou la juridiction qui souhaite s'y référer. La Commission des Nations Unies pour le droit commercial international (CNUDCI) «joue un rôle important dans la mise en place de ce cadre conformément à son mandat qui est d'encourager l'harmonisation et la modernisation progressives du droit commercial international» (Nations Unies, 2013). Elle énumère les instruments qui sont le plus souvent le résultat pour la réalisation de ces initiatives: des techniques et dispositifs législatifs (ex.: des conventions, des lois types; des guides législatifs et recommandations; des dispositions types); des techniques contractuelles (des clauses ou règlements qui peuvent être utilisés lors de la rédaction de contrat); et des techniques explicatives (ex.: des guides juridiques; des guides pratiques et autres guides d'information; et des déclarations interprétatives). La Commission est donc une source importante pour une initiative telle quelle.

Néanmoins, il existe toujours plusieurs intérêts et les inquiétudes que nous devons évoquer lors de la création de telles initiatives. La protection des données privées, la circulation libre de l'information, l'efficacité, le commerce international et l'enquête sur le cybercrime (cybercriminalité) sont quelques-uns parmi plusieurs intérêts et/ou inquiétudes qui sont posés à l'égard des lois d'harmonisation. Par exemple, l'OECD note qu'il est important de maintenir un équilibre entre la protection des données et la circulation libre de l'information, étant donné qu'une pauvre circulation de l'information peut avoir des effets significatifs sur le commerce international. Comme nous pouvons le constater, il existe un lien évident entre les instruments, les acteurs et les intérêts mutuels qui rassemblent les deux. C'est en identifiant et clarifiant les relations entre les instruments, les acteurs et les intérêts que nous sommes en mesure de comprendre le but de chaque instrument, de juger si celui-ci va réussir à répondre aux besoins pour lesquels il a été conçu, et enfin d'identifier les lacunes, ainsi que les instruments qui sont toujours manquants.

Enfin, il existe plusieurs théories, principes et concepts quant à l'harmonisation des lois: par exemple la règle de la territorialité; le principe de la nationalité; le principe du drapeau; le principe de la responsabilité; le principe d'adéquation; le principe du détenteur du fichier/responsable du traitement; et le principe du pouvoir de disposition. D'après les lectures, il reste toujours à répondre à quelques questions: qui se sert de ces théories/principes/concepts? Dans quel contexte? Comment et avec quelle intention? Sont-ils opposés ou complémentaires l'un de l'autre? Est-ce qu'il existe un lien entre ces théories/principes/concepts et les instruments/acteurs/intérêts et/ou inquiétudes? Bref, l'idéal serait d'identifier laquelle de ces théories serait le/la plus utile aux fins de ce projet et de cette initiative. La création d'une carte d'harmonisation, à l'égard du Cloud computing, est un exemple d'un produit cohérent qui pourrait être le résultat de cet exercice. Ceci nous permettrait de continuer à identifier les lacunes, ainsi que les moyens de leur remédiation, en plus d'éliminer le redoublement des efforts et l'empiètement sur les initiatives de recherches d'autres organisations.

Les lois qui se rapportent au commerce international, notamment celles qui se rapportent aux avions et aux navires sur les mers et les espaces aériens internationaux, peuvent eux aussi servir d'exemples pour la rédaction d'une convention qui ferait question de la

manipulation, la circulation et l'hébergement des données dans le Cloud. Par exemple, les lois maritimes et aériennes internationales énoncent qu'un navire/avion doit être enregistré sous la nationalité d'un État en particulier; ceci entend donc que le navire/l'avion fait sujet des lois et des règlements de cet État et l'État est donc responsable du navire/de l'avion. Est-ce possible d'enregistrer un Cloud, y compris ses serveurs et les données qu'ils hébergent, à un État fixe? Si oui, quelle partie du Cloud (le type de service, le type de Cloud, ou le fournisseur tout compris) et à quel niveau (les données spécifiques d'un client ou tout un serveur)? Peut-on obliger un Cloud à limiter l'hébergement de ses serveurs au sein d'un État fixe?

Certaines lois sur le commerce international incluent aussi les notions du contrôle et des responsabilités de l'État du pavillon (*flag state*), de l'État côtier (*coastal state*) et de l'État du port. Déjà, un navire devait choisir de s'enregistrer au sein d'un État spécifique et c'était donc en tant que navire du pavillon qu'il aurait l'autorité de contrôle compétent. L'État du pavillon exerçait en raison un contrôle juridique, administratif et social sur le navire. Certaines lois changèrent avec le temps afin d'accommoder certaines insuffisances: par exemple, certains États du pavillon étaient dépourvus de ressources qui leur permettaient d'exercer un contrôle adéquat sur les navires du pavillon. Donc, ces nouvelles lois (ex. *Law of the Sea Convention*, 1982) accordèrent plus de pouvoir aux ports maritimes, leur permettant de mener une enquête sur un navire se retrouvant dans leurs ports par l'entremise d'une organisation internationale ou par voie diplomatique. La Grande-Bretagne a été parmi les premiers à exercer un tel pouvoir qui se serait traduit sous forme de journal des «navires contrevenants»; on remarque des similitudes entre ces types de lois et la manière dont s'y prend la Grande-Bretagne pour évaluer l'état de la gestion de l'information au sein du secteur public, ceux-ci étant d'abord assujettis au *Public Records Act* (1958) de la Grande-Bretagne[2].

Si on appliquait donc les mêmes règlements au sein des fournisseurs Cloud, ceci entendrait que les fournisseurs seraient assujettis à des inspections par des autorités de règlementations qui évalueraient jusqu'à quel niveau un fournisseur tel quel respecte des critères et/ou des standards internationaux, par exemple. Ceux n'ayant pas rencontré certains critères ou ayant connu un incident de violation de confidentialité des données pourraient être placés sur une liste de «fournisseurs contrevenants», ainsi affaiblissant la réputation de ce fournisseur. Cette information, circulée librement, permettrait donc aux utilisateurs de prendre des décisions en connaissance de cause. Et quant à l'État du pavillon, l'État côtier et l'État du port, serait-il possible d'imposer de telles notions sur l'environnement Cloud? C'est-à-dire, serait-il possible d'obliger à ce que les fournisseurs du Cloud s'enregistrent au sein d'un État spécifique qui, à son tour, veillerait sur ce fournisseur? La nature du Cloud implique un besoin pour des règlements et des lois de nature internationale s'il y a l'espoir que le Cloud soit règlementé de façon uniforme au-delà des frontières dont lui-même n'en est pas sujet.

La protection des données en Europe

Selon le bureau d'avocat White & Case, la protection des données privées n'est pas règlementée de manière aussi détaillée aux États-Unis qu'elle l'est ailleurs (p. ex.: l'Union européenne; Canada; Australie; etc.) (White & Case LLP, 2009). L'Union européenne en particulier a les lois les plus sévères quant à la protection des données privées. Il existe plusieurs initiatives en Europe quant au Cloud computing. Celles-ci, menées par la Commission européenne, sont faites en conformité avec le Data Protection Directive qui tient compte de la gestion et surtout de la protection de l'information privée et des données électroniques, y

[2] Cet acte entend qu'une agence du secteur public doit gérer son information d'après la section 46 du *Freedom of Information Act* (2000).

compris l'information de nature privée qui est gérée ou hébergée dans le Cloud. On compte parmi ces plus grands succès jusqu'à présent la publication de textes clés[3] se rapportant au Cloud et l'initiation du groupe de travail «Article 29», ou le groupe de travail sur la protection des données.[4] Ces succès sont le résultat d'un groupe de travail sur la Stratégique du Cloud computing de la Commission européenne qui mène diverses initiatives et projets de recherche et qui a comme buts: la création de lois et de règlements modèle qui seraient exerçable au niveau de la rédaction d'accords et de contrats à niveau de service; l'identification de standards nécessaires et l'élimination de standards superflus; et l'établissement d'un *European Cloud Partnership* qui est responsable de la création d'exigences d'acquisition communes quant au Cloud computing (*Cloud Computing Strategy*). Nous comptons parmi ces plus grandes initiatives la présentation du *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (*General Data Protection Regulation*) en 2012, qui entend l'établissement de règlements propres à la gestion des données personnelles d'une manière uniforme pour les 27 États-membres; en cas de succès, ça serait le premier de son genre.

D'autre part, la revue de littérature a compris plusieurs études de cas de la mise en œuvre du Cloud, dont ceux-ci présentant souvent des exemples de cas réussis. En revanche, il existe peu d'études empiriques qui tracent la perspective de l'utilisateur. C'est donc cette constatation qui a mené à la création du questionnaire sur le Cloud qui cible spécifiquement les utilisateurs.

Synthèse des écrits sur l'avancement de la pratique du Cloud au niveau international et au niveau suisse

Le concept du Cloud computing s'est révélé relativement récemment. Cependant, il semble prendre une place de plus en plus prépondérante dans le domaine public et privé depuis quelques années. Cette constatation paraît s'affirmer alors que l'expansion future de ce service se concrétise toujours davantage. Basée sur l'observation du marché, cette réflexion doit être confirmée ou infirmée par des données fiables. Dans ce but, nous avons identifié dans la littérature professionnelle six études qui ont cherché à évaluer la maturité des pratiques du Cloud computing dans les entreprises suisses et internationales. Dans ce chapitre, nous décrirons pour chacune des six études la méthode de recherche, ainsi que le champ d'application choisi d'une part, et d'autre part les résultats qui nous ont paru les plus significatifs.

La première étude que nous avons sélectionnée est une enquête menée par l'institut de recherches indépendant *Kelton Research* sur mandat de l'entreprise américaine *Avanade*, une

[3] En voici quelques exemples: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe*; *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, [2012] OJ C 102/55*; *Commission Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,[1995] OJ, L281/31*.

[4] Le groupe publia « *Opinion 08/2010 on Applicable Law* » en 2010 et « *Opinion 05/2012 on Cloud Computing* » en 2012.

filiale de la multinationale *Accenture* (Séverin, 2011)**.** Plus de 570 membres issus de la direction, des managers et des responsables IT provenant de Suisse et de 17 autres pays ont été interrogés. Les résultats publiés en novembre 2011 révèlent notamment qu'un tiers des entreprises basées en Suisse dépense entre 20 % et 30 % de leur budget IT pour leur service de Cloud computing. Par ailleurs, à cette époque, 68 % des entreprises provenant d'Europe ont déclaré utiliser des services Cloud, alors que ce chiffre ne s'est élevé qu'à 33 % en Suisse. L'enquête a également mis en avant le fait que 20 % des participants implantés en Suisse ont connu des problèmes liés à l'utilisation non maîtrisée de services Cloud. Le même pourcentage des sondés relève qu'il n'existe pas de dialogue entre les responsables IT et les départements métier qui souscrivent ou utilisent des services Cloud de leurs propres initiatives (alors que le chiffre au niveau mondial atteint 27 %). Enfin, une comparaison avec l'étude d'*Avanade* sur le Cloud computing réalisée en janvier 2009 montre une nette augmentation de l'acceptation des services Cloud au niveau mondial. Ainsi, il y a deux ans, 39 % des entreprises recouraient au Cloud, un chiffre qui s'élève aujourd'hui à 74 %. En Suisse, ce chiffre est passé de 30 à 33 %.

La deuxième étude a été effectuée par l'entreprise de consulting informatique suisse *Cambridge Technology Partners*, en 2011 également. Cette enquête, qui a duré quatre mois, eut pour but d'évaluer le niveau d'intérêt, de préparation et d'activité du Cloud computing au sein des entreprises basées en Suisse. La majorité des sondés regroupe des managers issus dans le deux tiers des cas d'entreprises employant plus de 1000 personnes. Les résultats indiquent que 70 % des participants confirment que le Cloud computing représente une option technologique viable qui aura pour conséquence de restreindre la taille du département informatique. Si 42 % des interviewés confirment que leur organisation utilise d'ores et déjà le Cloud computing, la quasi-unanimité (95 %) affirme que leur institution à l'intention d'augmenter l'utilisation de ce concept dans un futur proche. Cela s'explique notamment par le fait que 90 % des organismes ayant introduit le Cloud computing estiment que ce choix fut un succès. Cependant, selon 71 % des participants, le principal frein à cette expansion proviendrait de la culture interne de l'entreprise.

L'étude menée en mars 2013 par *T-Systems*, une entreprise allemande spécialisée en informatique et dans les télécommunications appartenant au groupe *Deutsche Telekom*, constitue la troisième source (Lelièvre, 2013). Il s'agit d'une enquête annuelle réalisée auprès des entreprises suisses sur le thème des stratégies d'achat et TIC. Il en ressort que 44 % des institutions approchées jugent le Cloud computing pertinent. En effet, 40 % des applications commerciales, 30 % des outils de messagerie et 34 % des sauvegardes s'effectuent à partir du Cloud.

La quatrième publication met en avant une étude conduite en 2013 par *Analysys Mason*, une entreprise internationale experte dans les télécommunications, les médias et la technologie (Brodard, 2013). Il en résulte que le marché global du Cloud public devrait atteindre 31,9 milliards de dollars en 2017, alors qu'il s'est élevé 18,3 milliards en 2012. En Suisse, le marché passera de 139 millions de dollars en 2012 à 249 millions en 2017, soit une progression annuelle de 12.35 %. Ce sont les petites organisations, entre 10 et 49 employés, qui présentent le plus de potentiel de dépenses dans ce domaine avec 15.6 % de progression, suivies par les sociétés de taille moyenne (12.8 %).

Pour sa part, l'entreprise d'analyse du marché informatique suisse *MSM Research* a exploré plusieurs études sur les tendances informatiques en Suisse (Badel, 2014). Les résultats, publiés en juillet 2013, démontrent que 39 % des entreprises escomptaient réaliser des économies en 2013 et 65 % pensaient y arriver d'ici 2015, grâce au Cloud computing. Cette

projection aurait poussé 22 % des institutions à opter pour ce service et même à accélérer le processus de migration des données dans cette direction.

Enfin, une enquête effectuée par le développeur *Alfresco Software* en 2013 et portant sur le marché international expose que sur 1600 managers provenant de 8 pays (États-Unis d'Amérique, Royaume-Uni, France, Japon, Allemagne, Espagne, Inde et Italie), 82 % des interrogés souhaiteraient intégrer le Cloud computing dans leur institution (Alfesco Software, 2013).

Questionnaire avec les utilisateurs

Le projet RiC a donc choisi de poursuivre son propre questionnaire au niveau des utilisateurs. Le questionnaire, qui a connu plusieurs révisions, a compris un total de 34 questions dans sa version finale. Le but du questionnaire fut d'obtenir des renseignements généraux de la part des utilisateurs – courants, anciens et potentiels – quant à leur perspective et/ou leur opinion sur le Cloud. Il était question aussi d'examiner le niveau de maturité de ces utilisateurs par rapport aux pratiques Cloud et de voir quelles étaient leurs craintes d'une part et leurs motivations d'autre part envers les différentes options offertes par le Cloud.

Le questionnaire inclut des questions se rapportant aux risques du Cloud, aux incitatifs qui poussent un groupe à confier leurs données dans le Cloud, aux modèles de services et de déploiements, aux problèmes rencontrés avec le Cloud, et aux contrats de service. Des questions additionnelles ont été incluses afin d'assurer que les réponses reflétaient plutôt une perspective du Cloud au niveau organisationnel et non une perspective individuelle. Entre autres, toutes les questions ont été conçues de manière à encourager les répondants à partager leurs expériences en matière de Cloud avec nous.

Le questionnaire a permis de collecter des résultats significatifs. En avril 2013, le questionnaire fut distribué en Amérique du Nord pendant environ un mois par l'entremise de listes de diffusion courriel (misé vers la gestion de l'information et l'archivage) et de médias sociaux (*LinkedIn*, *Facebook* et *Twitter*). Il eut un total de 353 répondants, dont la majorité fut des gestionnaires de données (26 %) ou des archivistes (22 %), d'entreprises gouvernementales (30 %) ou éducatives (36 %), dont la majorité de grande taille (+500 employés) (49 %). Les résultats significatifs tirés de l'analyse du questionnaire furent les suivants:

- On observe une augmentation sur le plan de l'utilisation du Cloud et que le nombre de gens considérant se déplacer vers le Cloud est toujours impressionnant. Le questionnaire a montré que 57 % des répondants se servent présentement du Cloud, dont la majorité d'entre eux s'en servent depuis au moins trois ans; 38 % des répondants considèrent potentiellement un déménagement vers Cloud;

- Le département informatique (IT) était responsable pour la gestion du Cloud pour 61 % des entreprises ayant adopté le Cloud. Seulement 19 % des utilisateurs courants ont nommé les gestionnaires de l'information et des données en tant que responsable.

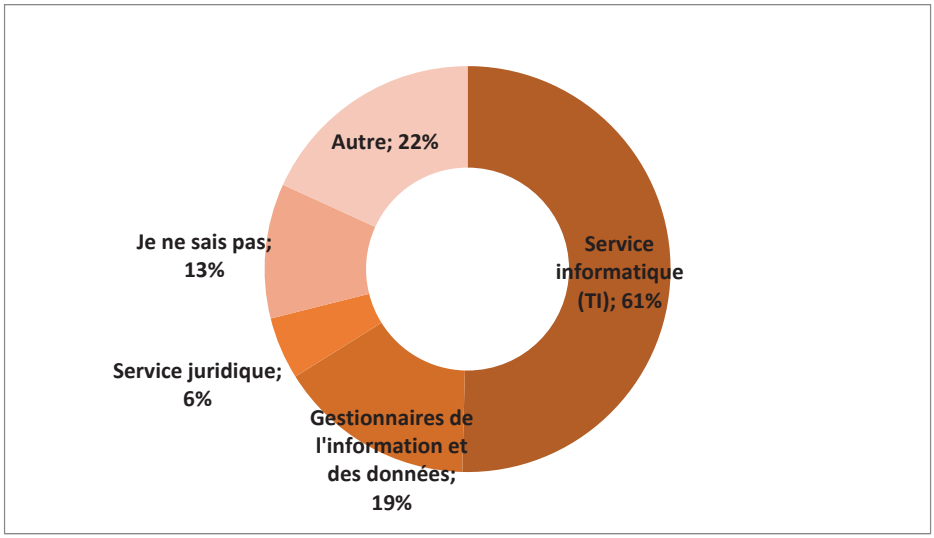

Fig 1 Résultats de réponses pour la question «Quel(le) unité/département est responsable pour la gestion du Cloud au sein de votre entreprise?»

- Un nombre élevé d'utilisateurs courants (54 % des répondants qui se servent du Cloud) ainsi que les utilisateurs potentiels (58 % des répondants n'utilisant pas le Cloud) sont motivés par le coût réduit du Cloud; cependant, certains d'entre eux remarquent que c'est un bénéfice qui n'est pas toujours facile à tirer.

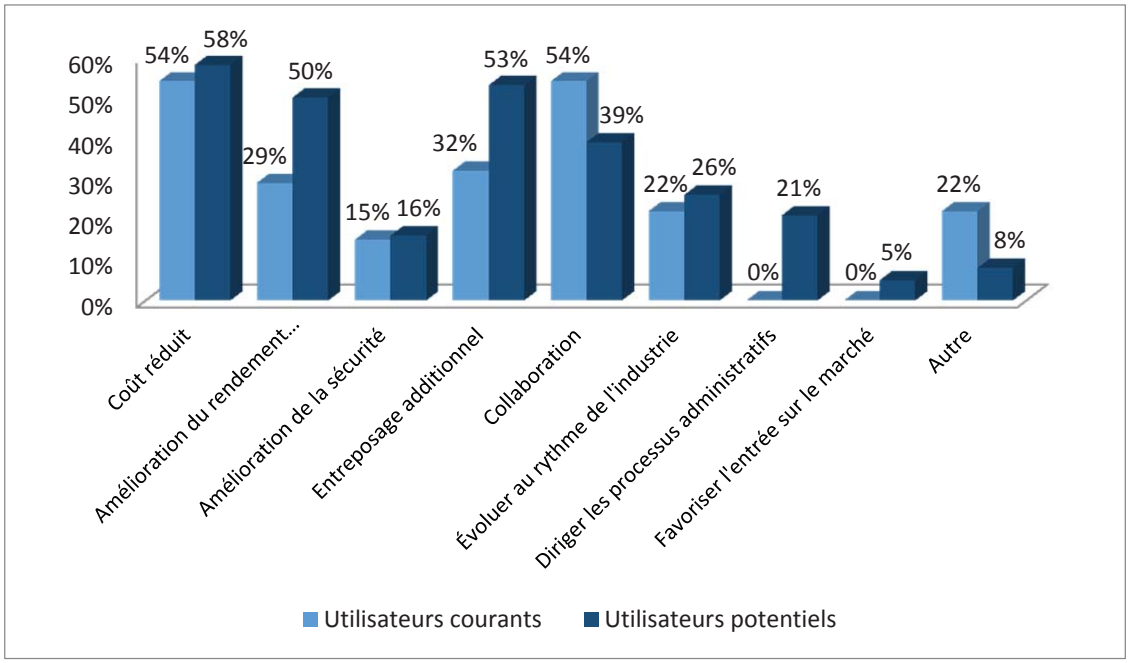

Fig 2 Comparaisons des raisons pour laquelle les utilisateurs courants on choisit d'adopter le Cloud et les raisons pour laquelle les utilisateurs potentiels considèrent adopter le Cloud.

- Seulement une petite portion d'utilisateurs courants a profité d'un accord de service (SLA) ou de mesures semblables afin de se protéger contre les risques que peut présenter le Cloud. Parmi les répondants qui ont été parmi ceux qui ont pris la décision de se déplacer vers le Cloud, seulement 35 % d'entre eux ont négocié un accord de service (SLA).

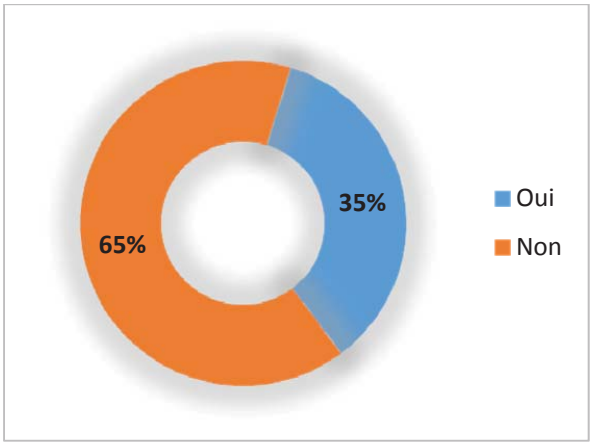

Fig 3 Résultat de réponses à la question «Avez-vous négocié un accord de service avec le fournisseur du Cloud?»

- Les problèmes posés par le Cloud ne se rapportent pas toujours à la technologie, mais peuvent aussi comprendre la gestion de l'organisation, le comportement humain (par exemple, une perte de contrôle sur l'utilisation du Cloud par les employées), les règlements (par exemple, un manque de règlements stricts entourant l'utilisation adéquate du Cloud), la gestion des données, des difficultés rencontrées lors de la mise en œuvre de l'outil, et un manque de transparence de la part des fournisseurs.

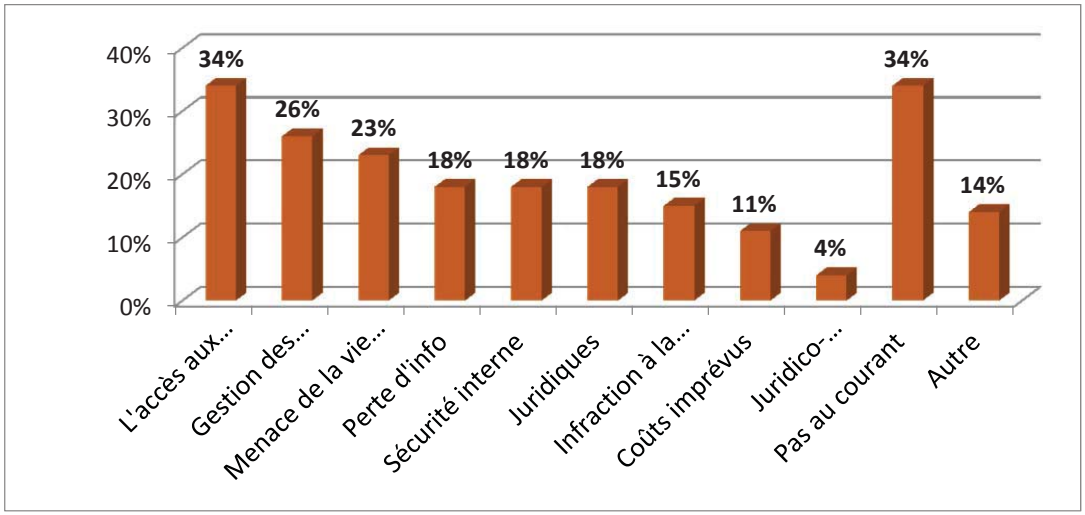

Fig 4 Résultats de réponses à la question «Quels sont les problèmes que vous avez rencontrés avec le Cloud?»

- Le risque pour la sécurité des données dans le Cloud est toujours parmi les raisons qui empêchent certains groupes d'adopter le Cloud; 56 % des répondants qui ne considéraient pas le Cloud ont tous exprimé ce même ennui. Les «répercussions juridiques», «la perte de contrôle sur les données» et «le risque à la vie privée» ont aussi été parmi les réponses les plus populaires.

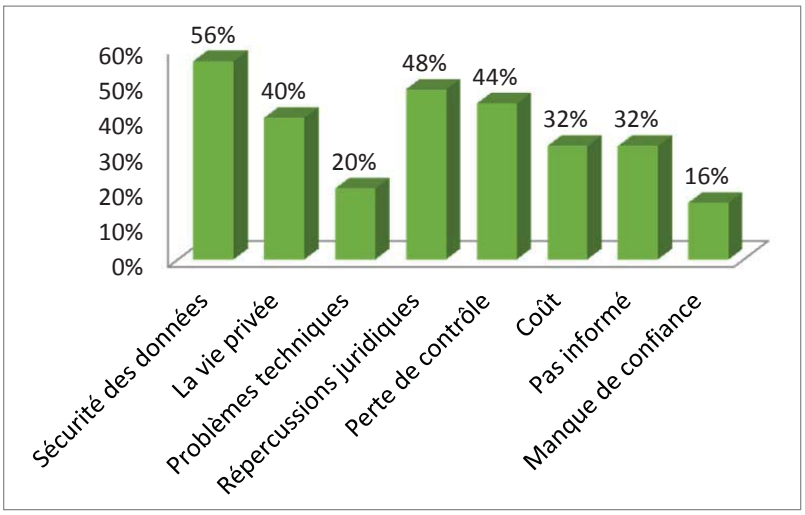

Fig 5 Résultats de réponses à la question «Quelles sont les inquiétudes Principales qui vous empêchent d'utiliser le Cloud?»

- Les services du Cloud varient entre les utilisateurs courants et les utilisateurs potentiels; alors que plusieurs des utilisateurs courants ont opté pour le Cloud public, les utilisateurs potentiels ont tendance à s'orienter plutôt vers le Cloud privé.

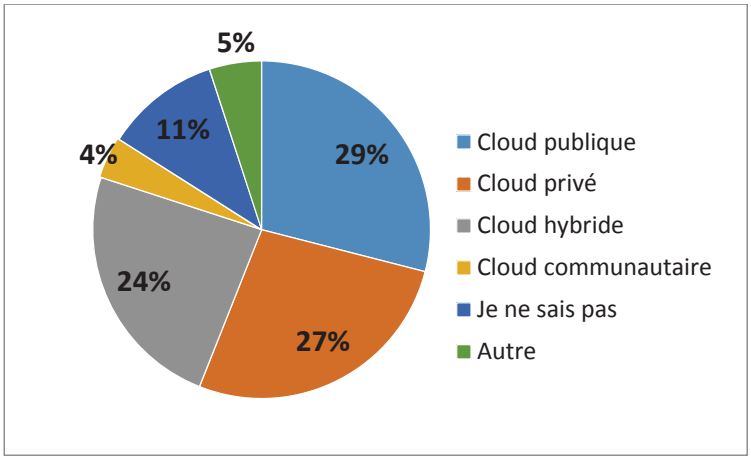

Fig 6 Résultats de réponses de la question «Quel est le type de Cloud dont vous vous servez dans votre entreprise?»

De manière générale, les résultats du questionnaire ont permis d'identifier et de comparer divers types d'utilisateurs – courants et potentiels – du Cloud qui, en soi, a permis d'acquérir une connaissance de l'état actuel de l'utilisation du Cloud. Certaines conclusions tirées de l'analyse des réponses au questionnaire ont été conformes aux conclusions tirées de la revue de la littérature effectuée dans le cadre du projet. En premier instant, il fut conclu que l'incitatif le plus important pour ceux considérant un déménagement vers le Cloud est le coût, et la majorité des utilisateurs courants du Cloud et de ceux ayant déjà utilisé le Cloud ont opté pour le SaaS du Cloud. Toutefois, ceux souhaitant de profiter du coût raisonnable du Cloud doivent souvent souscrire à des services de bas niveau, posant parfois des problèmes imprévus. La résolution de ces derniers entend souvent des coûts également imprévus. D'ailleurs, les résultats du questionnaire ont aussi révélé que les facteurs imprévus ne sont pas uniquement techniques, mais peuvent parfois même être influencés par le mode de gestion de ces services Cloud. Pour tous les utilisateurs par contre, la sécurité et la protection des données sont les facteurs qui inquiètent le plus les utilisateurs lorsqu'ils évaluent les risques du Cloud. Un rapport traitant des résultats et des conclusions tirées du questionnaire ou *User Survey Report* a été publié et peut être retrouvé sur le site web www.recordsinthecloud.com.

Entrevues avec les fournisseurs Cloud

Parallèlement au questionnaire en ligne envoyé aux utilisateurs (actuels ou possible des solutions Cloud), plusieurs entrevues semi-structurées ont été réalisées. Il s'agit plus précisément de huit entrevues réalisées jusqu'à aujourd'hui qui se répartissent comme suit: trois (3) entrevues en Suisse (Genève), quatre (4) entrevues en Amérique du Nord (Canada et États-Unis) et une (1) entrevue en Chine. L'échantillonnage de ces participants s'est fait par choix de cas pertinents. Les participants sont tous des fournisseurs de divers services et solutions Cloud. Les huit (8) entrevues ont été menées par différent(e)s chercheur(e)s du projet RiC et les données ont été collectées selon le même guide d'entrevues. Ce dernier a été utilisé dans trois langues: en français pour les entrevues réalisées avec les participants suisses, l'anglais pour les participants de l'Amérique du Nord, et en mandarin pour le participant de la Chine. L'objectif de ces entrevues semi-structurées fut d'explorer le point de vue des fournisseurs du Cloud sur la question de la confidentialité des données, de leur rétention, destruction et de l'intégration du calendrier de conservation, de leur stockage et de leur protection, de leur authenticité et des différents risques légaux à l'égard de conditions de recevabilité, techniques et managériaux qui menacent leurs caractères probants, leur accessibilité et leur pérennité. Le traitement des données de ces entrevues est en cours. D'autres entrevues semi-structurées seront poursuivies les prochains mois.

Jusqu'à présent, nous pouvons faire certains constats d'après les résultats préliminaires tirés des entrevues avec ces fournisseurs. D'abord, nous constatons que les fournisseurs répondent de manière adéquate aux inquiétudes de leurs utilisateurs, surtout aux questions de la sécurité des données dans le Cloud, l'accès aux données, l'emplacement et la localisation des données, et la négociation des accords de données. D'ailleurs – et peut-être bien entendu – , nous n'avons enregistré aucun cas d'erreurs, de mauvaise gestion, de perte de données ou de bris/d'infraction à la sécurité de leur(s) Cloud(s). Selon les fournisseurs, ils se comportaient selon les normes et les standards de l'industrie. Donc, nous sommes plutôt en mesure de souligner ce qui n'a *pas* été adressé lors de ces entrevues; les questions portant sur la gestion des données, l'authenticité et l'intégrité des données et des métadonnées posées dans le Cloud. D'ailleurs, ce sont des questions et des inquiétudes qui n'ont pas été posées ni par les

fournisseurs, ni par les utilisateurs. C'est d'ailleurs un sujet qui mériterait d'être exploré davantage et de manière approfondie si nous souhaitons comprendre les risques et les bénéfices que posent la gestion des données et de l'information dans le Cloud.

Nous avons aussi constaté qu'il existe une fracture entre les fournisseurs du Cloud européens et les fournisseurs nord-américains. Les participants européens étaient prêts au dialogue; ils étaient heureux de nous apprendre des mesures de sécurité qu'ils avaient élaborées au sein de leur entreprise pour satisfaire aux besoins de leur clientèle et des normes de l'industrie. Ils nous ont même invités à visiter les sites où ils stockent les données de leurs clients. Au contraire, les fournisseurs nord-américains se sont montrés réticents à s'engager dans un dialogue trop détaillé, surtout quant aux questions touchant à la spécificité des mesures de sécurité qu'ils ont en place pour assurer la protection des données et de leurs serveurs Cloud.

Prochaines étapes…

Le projet a d'abord l'intention d'élargir le champ du dialogue des utilisateurs; bien que le premier questionnaire ait ciblé une région spécifique d'utilisateurs du Cloud, le projet aimerait désormais s'étendre à d'autres régions de l'Europe et de l'Asie. Ceci a déjà été réussi – en partie – avec les fournisseurs du Cloud (en Suisse), mais le champ de recherche devrait être élargi pour inclure également les utilisateurs de régions semblables, offrant donc un bon aperçu des deux perspectives (utilisateurs vs fournisseurs) du Cloud. Bien que le champ de participants pour les entrevues avec les fournisseurs doit être élargi, il conviendrait peut-être également de considérer changer ou modifier le dialogue, soit de changer les questions posées ou bien le style de l'échange tout entier afin d'inciter un différent échange et donc des différents résultats quant à cette facette de la recherche. À cet égard, le projet cherche aussi à affiner et mieux cerner les besoins des utilisateurs. Les risques du Cloud et les inquiétudes que ceux-ci posent aux utilisateurs sont bien connus; cependant, comment réussissons-nous à les calmer? Quelles sont les attentes des utilisateurs envers le fournisseur pour réconcilier ces lacunes? Est-il possible de faire confiance au fournisseur et des données qu'on lui confie? Le projet aimerait explorer ces questions d'après la perspective des utilisateurs, de ceux qui ont une relation courante avec un fournisseur du Cloud, tout comme ceux qui envisagent un jour de se lancer dans le Cloud. Le projet cherche aussi à élargir sa base de données quant aux fournisseurs du Cloud et des services que ceux-ci offrent. Le but ultime de la recherche est d'établir un cadre pour un Cloud de confiance (*Trusted Cloud Framework*); définissant le rôle que les fournisseurs du Cloud ont à jouer afin d'accomplir cet objectif. Le *Cloud Security Alliance* (CSA) est un groupe qui préconise les bonnes pratiques quant à la sécurité des données dans le Cloud[5]; RiC tient à s'inspirer de leurs initiatives. CSA effectue des recherches sur comment améliorer la sécurité du Cloud et ainsi la relation entre fournisseur et utilisateur; jusqu'à présent, les résultats comprennent la distribution de module éducatif et de certification diverse.

[5] « *To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing*. »
Cloud Security Alliance, site web, https://cloudsecurityalliance.org/.

Menant plus d'une dizaine d'initiatives de recherche à la fois[6], le groupe reste à l'avant-garde de la gestion et de l'application de la sécurité du Cloud et des données qui lui sont confiées et ambitionne qu'un jour ceux-ci soient mandatés en tant que certification obligatoire pour les fournisseurs du Cloud. Comme le suggère le nom de notre projet, *Records in the Cloud* cherche donc à introduire une composante additionnelle à ces genres d'initiatives, une composante qui tient compte des données mêmes dans le Cloud. La conservation de l'authenticité et l'intégrité de ces données permet ensuite à ceux-ci et à l'information qu'ils communiquent d'être source fiable pour ceux qui s'y appuie; c'est une question qui est peu souvent discutée dans la littérature sur le Cloud. Le projet cherche donc à créer un cadre qui intègrera a la question de l'authenticité des données et de leur fiabilité, un ensemble de critères (sécurité, accès, contrôle, etc.) qui seront indispensables à la création d'un environnement Cloud fiable, en lequel l'utilisateur peut avoir confiance de protéger et bien gérer ses données. Pour le fournisseur qui cherche à accroitre ou renforcer la confiance que l'utilisateur courant et potentiel a dans ses produits et ses services, ce genre de structure est nécessaire et ce n'est pas exagéré de suggérer que ce sera bientôt une obligation.

Le projet InterPARES Trust (ITrust, http://www.interparestrust.org) a de son côté développé ces aspects liés à la sécurité des données en ligne qui reposent justement sur le contrôle de l'authenticité et de l'intégrité des données électroniques. De ce fait, des synergies ont été constatées entre le projet RiC et le projet ITrust. Le projet ITrust est une recherche internationale et interdisciplinaire qui vise à produire des dispositifs via un réseau de chercheurs, d'experts et de partenaires au niveau local, national et international. Ces dispositifs consisteront en un ensemble de politiques, de procédures, de règlements, de normes concernant les documents numériques sur internet. L'objectif ultime du projet ITrust est d'augmenter la confiance du public en la gestion des données en ligne en favorisant non seulement la démonstration et la traçabilité de la bonne gouvernance de celles-ci, mais également la pérennité de la mémoire numérique et de son accessibilité. Le projet RiC sera alimenté grâce à des collaborations fructueuses avec les études menées et planifiées par les diverses équipes de recherche du projet ITrust. Avec son réseau étendu sur tous les continents et ses nombreux partenaires institutionnels, académiques et professionnels, le projet ITrust contribuera à l'avancement de la suite de la collecte de données du projet RiC et enrichira l'analyse et l'interprétation de ces dernières. Les résultats du projet ITrust portant spécifiquement sur le cloud seront en-soi complémentaires au projet RiC.

Dans cet ordre d'idée, le projet RiC profitera aussi des résultats de la recherche QADEPs (Définition et mesure des qualités des archives et documents électroniques): une recherche récente menée par la professeure Makhlouf Shabou (2013) de la Haute école de gestion de Genève sur la mesure des dimensions de qualité des données et archives électroniques publiques dans les institutions publiques. Le premier objectif de cette étude était de concevoir un cadre conceptuel définissant les principales dimensions et indicateurs des qualités des archives électroniques. Le deuxième objectif consistait à développer des variables permettant d'évaluer sur des échelles de mesure les dimensions et indicateurs définis précédemment. Quatre sous-objectifs ont guidé l'élaboration de ces variables:

[6] *CSA Security Guidance* (V3.0) : *Security Guidance for Critical Areas of Focus in Cloud Computing Foundational best practices for securing Cloud computing* ; *Cloud Controls Matrix* (CCM); *Consensus Assessments Initiative* (CAI); *Cloud Audit*; CloudCERT; *Trusted Cloud Initiative* (TCI), *GRC Stack*; *Cloud Trust Protocol* (CTP); *Health Information Management* (HIM); *Cloud Data Governance* (CDG); *Security as a Service* (SecaaS); *Top Threats*; *Telecom Working Group* (TWG); *Innovation Initiative* (CSA Innovate); *Mobile Working Group* (CSA Mobile); *Open Certification Framework* (OCF); *Privacy Level Assessment* (PLA); *Incident Management and Forensics* (IMF); et *Legal Information Center* (CLIC).

1. favoriser les dispositifs automatisables, ce qui présente un avantage indéniable pour le traitement de données extrêmement abondantes;
2. limiter le caractère subjectif des évaluations autant que possible;
3. documenter l'application des variables afin de rendre le fruit de cette étude aisément réutilisable et adaptable;
4. confirmer l'applicabilité et la pertinence des variables définies via des tests dans plusieurs institutions.

À travers une revue de la littérature menée en profondeur, le projet QADEPs a permis l'élaboration d'un cadre conceptuel décrivant les différents aspects de la qualité des archives électroniques de manière exhaustive.

Fondé en particulier sur des normes internationales et une recherche doctorale[7] sur le sujet, ce cadre conceptuel constitue une base solide pour toute réflexion menée sur la qualité des archives électroniques. Quant aux variables définies pour mesurer concrètement cette qualité, leur applicabilité a été confirmée pour l'ensemble d'entre elles à travers des tests réalisés aux Archives de l'État du Valais et aux Archives de l'État de Genève. L'ensemble des outils développés, validité et approuvés dans le cadre de ses tests permettent à toute institution gérant des archives publiques à des fins de conservation pérenne d'analyser la qualité des documents dont ils ont la charge. Un tel outil systématique et simple d'application n'existait pas avant ce projet. De plus, cet outil est modulable dans la mesure où il permet l'utilisation partielle et ciblée des variables et des mesures des qualités des archives électroniques, selon le besoin et les moyens à disposition.

Le modèle QADEPs analyse la qualité des archives électroniques des institutions publiques à travers trois dimensions: la «preuve crédible», l'«exploitabilité» et la «représentativité». Il subdivise ces dernières en 8 dimensions regroupant 17 indicateurs pour un total de 46 variables. Cette richesse permet de couvrir l'ensemble des aspects les plus importants de la qualité. Un travail important a également été réalisé autour du caractère automatisable de la mesure des variables: il en est ressorti que 60 % environ pouvaient être analysées à l'aide d'algorithmes. Plus spécifiquement, les résultats du projet QADEPs concernant la mesure de la fiabilité et de l'authenticité renforceront la réflexion que nous menons dans le cadre du projet RiC. L'identification de métriques précises, traçables, contrôlables et éventuellement automatisables offre une réponse logique et défendable aux utilisateurs du Cloud qui se posent des questions liées à la sécurisation de leurs données. Ceci permet d'avoir des éléments pertinents qui pourraient alimenter la réflexion sur les exigences techniques et les principales qualités et caractéristiques qu'il faut contrôler surtout s'il s'agit de gérer et/ou de stocker des données selon des solutions Cloud.

[7] Étude sur la définition et la mesure des qualités des archives définitives issues d'une évaluation. La thèse de doctorat est disponible au https://papyrus.bib.umontreal.ca/xmlui/handle/1866/4955. Voir aussi, B. M. Shabou, 2011, Measuring the quality of records to improve organizational documentary testimony, *Professional Communication Conference (IPCC), 2011 IEEE International*, Oct 17-19: 1-6, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6087223.

Conclusion

Comme précisé, le projet Records in the Cloud (RiC, http://www.recordsinthecloud.org/) vise à identifier et à analyser en profondeur les questions techniques, opérationnelles, juridiques et économiques relatives au traitement et à la conservation externalisée moyennant des options Cloud. Le facteur le plus attrayant pour les consommateurs intéressés au Cloud est l'éventuelle économie résultant de la réduction des coûts de la gestion des données. Contrairement à une infrastructure interne, l'achat des options et services Cloud implique que le coût du matériel et du logiciel – qui serait autrement géré par le consommateur – est absorbé par le fournisseur du Cloud; le consommateur n'a donc pas à s'inquiéter de la gestion de son infrastructure. L'élasticité du Cloud permet au consommateur une facilité d'utilisation s'il souhaite augmenter ou diminuer le niveau de service ou les ressources qu'il reçoit du fournisseur. Cependant, ce qui est présenté comme un «avantage» du Cloud peut aussi être perçu comme un risque. La renonciation du système traditionnel – de l'infrastructure interne – peut aussi être synonyme d'une renonciation de contrôle. L'achat du Cloud, réalisé selon un accord de service (SLA), exige que le consommateur exerce une diligence raisonnable; ces services comprennent chacun un certain niveau de sécurité, d'accès et de disponibilité, en plus d'espace et de *lieu* de stockage des données et de partage de contrôle entre consommateurs et fournisseur. Ceci ainsi augmente ou diminue le coût du Cloud; c'est-à-dire que si le consommateur souhaite exercer un plus haut niveau de contrôle sur certaines caractéristiques du Cloud – sur la sécurité des données, la disponibilité des données ou l'habileté de manipuler et personnaliser l'infrastructure, par exemple – il doit assumer les conséquences – ou le prix –, pour ainsi dire.

Les prochaines étapes de notre recherche clarifieront ces divers aspects. D'autres publications et conférences suivront également pour rapporter et partager les résultats intermédiaires et finaux du projet RiC.

Bibliographie

AHAMED, S. I. et M. SHARMIN. 2008. A trust-based secure service discovery (TSSD) model for pervasive computing, Computer Communications, 31(18): 4281-4293.

Alfresco Software. 2013. Connected Enterprise Survey Infographic (part 1). http://fr.slideshare.net/alfresco/2013-connected-enterprise-survey-infographic

ARAIZA, A. G. 2011. Electronic Discovery in the Cloud. Duke Law & Technology Review, 10: 1-19.
Article 29 Data Protection Working Party. 2012. Opinion 05/2012 on Cloud Computing. 01037/12/EN WP 196. http://idpc.gov.mt/dbfile.aspx/WP196.pdf.

Article 29 Data Protection Working Party. 2010. Opinion 08/2010 on Applicable Law. 0836-02/10/EN WP 179. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

ASHKOJ, J., S. SUGIMOTO et M. NAGAMORI. 2011. Preserving records in the cloud. Records Management Journal, 21(3): 175-187.

AUTONOMY, A. 2012. Best Practices for Cloud-Based Information Governance (White Paper). Network Systems Management. http://www.informationweek.com/whitepaper/Infrastructure/Network-Systems-Management/making-the-move-to-the-cloud-best-practices-adv-wp1347981072?articleID=191705703

BADEL, Pierre-Henri. *Aucune date*. Le cloud computing, tendance lourde de l'informatique. business-leader.ch. http://www.business-leader.ch/dossiers/47-informatique/2434-le-cloud-computing,-tendance-forte-de-l-informatique

BADGER, M. L., T. GRANCE, R. PATT-CORNER et J. M. VOAS. 2012. Cloud Computing Synopsis and Recommendations (NIST Special Publication 800-146). NIST: Gaithersburg, MD.

BASU, J. et V. CALLAGHAN. 2005. Towards a Trust Based Approach to Security and User Confidence in Pervasive Computing Systems. IEEE International Workshop on Intelligent Environments: 223-229.

BREUNING, P. et B. TREACY. 2012. Privacy, Security in Cloud Computing (Privacy and Security Law Report). Cloud Security Alliance, Information Systems Audit and Control Association. 2012 Cloud Computing Market Maturity Study Results: Rolling Meadows, IL.

BRODARD, Bastien. 2013. Suisse: le cloud public représentera 249 mios de dollars en 2017. ICTjournal. http://www.ictjournal.ch/fr-CH/News/2013/02/06/Suisse-le-cloud-public-representera-249-mios-de-dollars-en-2017.aspx

Cambridge Technology Partners. 2011. Le Cloud Computing en Suisse: Enquête sur l'utilisation du Cloud Computing par les entreprises en Suisse.http://www.market.ch/fileadmin/documents/market.ch/divers/octobre_2011/Enquete_CTP_sur_le_cloud_computing_aupres_des_entreprises_en_Suisse.pdf

CHUNG, H., J. PARK, S. LEE et C. KANG. 2012. Digital forensic investigation of cloud storage services. Digital Investigation, 9(2): 81.

Cloud Security Alliance [site web], https://cloudsecurityalliance.org/.

Commission européenne. Commission Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995. Official Journal L281, 23/11/1995 P. 0031 – 0050. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Commission européenne. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. 2012. COM/2012/010 final. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT.

Commission des Nations Unies pour le Droit Commercial International. 2013. Guide de la CNUDCI: L'essentiel sur la Commission des Nations Unies pour le droit commercial international. Vienne, Nations Unies. http://www.uncitral.org/pdf/french/texts/general/12-57492-Guide-to-UNCITRAL-f.pdf.

CUNNINGHAM, P. 2010. IT's Responsibility for Security. Compliance in the Cloud. Information Management, 44(5): 6.

DUBOURG, C. 2014. Archivage sur le cloud pratiques et perspectives (White paper). http://www.aproged.org/aprogedv2/index.php/espace-de-telechargement-aproged/lb-archivage-cloud-aproged.

FAN, W., S. YANG, J. PEI et H. LUO. 2012. Building trust into cloud. International Journal of Cloud Computing and Services Science, 1(3): 115-122.

GELLMAN, R. 2009. Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing (A Report). World Privacy Forum, http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

GOLD, J. 2012. Protection in the Cloud: Risk Management and Insurance for Cloud Computing. Journal of Internet Law, 15(12): 24-28.

GRAY, A. 2013. Conflict of laws and the cloud. Computer Law and Security Review, 29(1): 58-65;

GROUNDS, A. et B. CHEESBRO. 2013. Cloud Control: eDiscovery and Litigation Concerns with Cloud Computing. Computer and Internet Lawyer, 30(9): 23-31.
HOGAN, M., F. LIU, A. W. SOKOL et T. JIN. 2011. NIST Cloud computing Standards Roadmap (Special Publication 500-291). National Institute of Standards and Technology: Gaithersburg, Maryland.

JANSEN, W. et T. GRANCE. 2011. Guidelines on Security and Privacy in Public Cloud Computing (Special Publication 800-144). National Institute of Standards and Technology; Gaithersburg, Maryland.

JULISCH, K. et M. HALL. 2010. Security and Control in the Cloud. Information Security Journal: A Global Perspective, 19(6): 299-309.

KARAGEORGOS, Georgios et Nadezheda SERTOVA (*administrateurs*). 2013. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe. CESE 1701/2012 - TEN/494. http://www.eesc.europa.eu/?i=portal.en.ten-opinions.24758.

KATZAN, H. 2010. On the Privacy of Cloud Computing. International Journal of Management and Information Systems, 14(2): 1-12.

KESAN, J., C. HAYES et M. BASHIR. 2013. Information privacy and data control in cloud computing: Consumers, privacy preferences, and market efficiency. Washington & Lee Law Review, 70(1): 341-472.

LELIÈVRE, Hélène. 2013. L'externalisation se démocratise dans les grandes entreprises suisses.. ICTjournal. http://www.ictjournal.ch/fr-CH/News/2013/03/28/Lexternalisation-se-democratise-dans-les-grandes-entreprises-suisses.aspx.

LI, J., X. CHEN, O. HUANG et D. S. WONG. 2013. Digital provenance: Enabling secure data forensics in cloud computing. Future Generation Computer Systems.

MAKHLOUF SHABOU, Basma. 2011. Étude sur la définition et la mesure des qualités des archives définitives issues d'une évaluation. Thèse de doctorat. Université de Montréal. http://hdl.handle.net/1866/4955.

MAKHLOUF SHABOU, Basma. 2011. Measuring the quality of records to improve organizational documentary testimony. IEEE International: Professional Communication Conference (IPCC), 17-19 Oct. 2011: 1-6.
MOHAMMEH, D. 2011. Security in Cloud Computing: An Analysis of Key Drivers and Constraints. Information Security Journal: A Global Perspective, 20(3): 123-127.

MUTHULAKSHMI, V., A. A. YASEEN, D. SANTHOSHKUMAR et M. VIVEK. 2013. Enabling Data Security for Collective Records in the Cloud. International Journal of Recent Technology and Engineering, 2(1): 163-167.

OSTRZENSKI, Victoria. 2013. Cloud computing and Risk: A look at the EU and the application of the Data Protection Directive to cloud computing. Infopreneurship Journal, 1, 1: 29-38.

PAN, Weimei, Joy ROWE et Georgia BARLAOURA. 2013. User Survey Report., v. 10.1 Records in the Cloud project; Principal Investigator: Luciana Duranti.

SÉVERIN, Tania. 2011. La prolifération des services cloud – un danger pour les entreprises suisses? ICTjournal. http://www.ictjournal.ch/fr-CH/News/2011/11/04/La-proliferation-des-services-cloud--un-danger-pour-les-entreprises-suisses.aspx?pa=1.

SHABEEB, H., N. JEYANTHI et N. IVENGAR. 2012. A Study on Security Threats in Cloud. International Journal of Cloud Computing and Services Science, 1(3): 84-88.

SHAIKH, R. et M. SASIKUMAR. 2012. Security issues in cloud computing: A survey. International Journal of Computer Applications, 44(19): 4-10.

SINGH, A. et M. SHRIVASTAVA. 2012. Overview of security issues in cloud computing. International Journal of Advanced Computer Research, 2(1): 41-45.

STUART, K. et D. BROMAGE. 2010. Current state of play: Records management and the cloud. Records Management Journal, 20(2): 217-225.

SUBASHINI, S. et V. KAVITHA. 2010. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1): 1-11.

Unité de pilotage informatique de la Confédération UPIC. 2013. Stratégie suisse d'informatique en nuage. Confédération suisse. [site web]. http://www.isb.admin.ch/themen/strategien/01603/index.html?lang=fr.

Unité de Stratégie Informatique de la Confédération (USIC). 2011. Stratégie Cloud Computing des Autorités Suisses (White Paper). Département Fédéral des Finances (DFF): Berne.

WANG, H., W. HE et F. WANG. 2012. Enterprise cloud service architectures. Information Technology & Management, 13(4): 445-454.

White & Case LLP. 2009. Global HR Hot Topic: Data Breach Notification and the Multinational Employer. New York, White & Case LLP. http://www.whitecase.com/files/Publication/86781709-3f0b-4d5c-89d9-8d639267495a/Presentation/PublicationAttachment/3617942c-94a8-4885-be20-a2a0b83952a4/Global_HR_September_2009.pdf.

ZISSIS, D. et D. LEKKAS. 2011. Addressing cloud computing security issues. Future Generation Computer Systems, 28(3): 583-592.