Septembre 2015

ACPPU Note de synthèse

Externalisation

Les administrateurs d'université et de collège confient de plus en plus à des tiers la fourniture des services TI dont leurs établissements ont besoin. Concrètement, ils remplacent leur système TI, leur serveur et leurs spécialistes TI sur place par des services offerts à distance par un fournisseur de services infonuagiques et ses employés. De nombreux établissements ont déjà transféré la prise en charge et la gestion des comptes de messagerie électronique des étudiants à de tels fournisseurs, et sont de plus en plus séduits par l'idée de stocker dans le nuage les courriels, les dossiers et les données du personnel académique.

La décision d'une université ou d'un collège d'externaliser un ou plusieurs services à des fournisseurs dans l'environnement infonuagique pourrait porter atteinte à la vie privée de tous ses employés et étudiants. L'établissement donne alors à un fournisseur tiers accès aux renseignements personnels et professionnels de ses employés, ou encore aux données personnelles et scolaires des étudiants, pour des utilisations secondaires. Tant les employés que les étudiants pourraient porter plainte en vertu des lois sur la protection de la vie privée et des renseignements personnels.

Les membres du personnel académique peuvent contester l'accès à leurs dossiers personnel et professionnel par des fournisseurs de services infonuagiques pour le motif qu'un tel accès enfreint le droit à la liberté académique et le droit à la vie privée qui leur sont conférés en vertu de leur convention collective et de lois d'application générale.

L'ACPPU offre son aide aux associations de personnel académique dans des établissements qui envisagent la possibilité d'externaliser les données de leurs membres à des fournisseurs de services infonuagiques ou qui opèrent la migration.

Qu'est-ce que l'infonuagique?

Pour simplifier à l'extrême, disons que l'infonuagique désigne la prestation de services de stockage, d'accès et de traitement pour des données et des programmes, sur Internet ou sur des réseaux externes plutôt que sur des disques ou des réseaux informatiques locaux. Le *National Institute of Standards and Technology* aux États-Unis en donne la définition suivante :

*L'infonuagique est un modèle informatique permettant un accès réseau omniprésent, pratique et à la demande à un bassin partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peuvent être fournies et activées rapidement en réduisant au minimum la gestion ou les contacts avec les fournisseurs**.
[Traduction]

En réalité, le nuage est un centre de données, habituellement un immeuble qui ressemble à un entrepôt rempli de serveurs. Il peut être situé à quelques kilomètres seulement de votre établissement, ou encore à des centaines, voire des milliers, de kilomètres de distance.

---

* National Institute of Standards and Technology, Special Publication 800-145, septembre 2011, *The NIST Definition of Cloud Computing*, point 2, page 2. On peut consulter cette publication à l'adresse http://1.usa.gov/1umXAe3.

CAUT ACPPU

Canadian Association of University Teachers
Association canadienne des professeures et professeurs d'université
www.acppu.ca

cope225sepb.ca

Quels sont les enjeux de l'infonuagique pour le personnel académique?

Un libre accès aux renseignements sur le personnel académique par un fournisseur de services infonuagiques commerciaux constitue, au sens de la convention collective et de la loi, une violation du droit à la liberté académique et du droit à la vie privée.

Le contrat liant l'université ou le collège et le fournisseur de services d'infonuagiques peut inclure une clause autorisant ce dernier à recueillir, à explorer et à stocker les données concernant les membres du personnel académique en prévision d'utilisations secondaires. En acceptant une telle clause, l'établissement donne en fait carte blanche au fournisseur pour créer des profils d'employé et tirer un avantage monétaire des données recueillies.

L'analyse des données est un secteur important et en plein essor, en constante mutation. Les nouvelles méthodes et les avancées technologiques cohabitent avec un manque de transparence quant à la manière dont les données sont traitées et commercialisées. Même si un fournisseur assure qu'il ne collectera pas de données pour envoyer de la publicité aux utilisateurs, ou bien des données d'utilisateur final pour mener des opérations de publicité ou de marketing, rien ne dit qu'il n'utilisera pas les données dans d'autres activités commerciales. Voilà pourquoi il est important que le contrat autorise le fournisseur à avoir accès aux renseignements sur le corps professoral uniquement aux fins de la prestation des services externalisés, c'est-à-dire pour protéger le système contre les logiciels malveillants ou pour en faire la maintenance générale, etc.

Les centres de données dirigés par des entreprises basées aux États-Unis sont soumis à la surveillance de l'Agence de sécurité nationale américaine, la NSA, et, par conséquent, les données sur le corps professoral qu'ils détiennent le sont également.

Les organismes de surveillance et d'application de la loi américains sont habilités à accéder aux courriels et aux divers documents stockés sur les grappes de serveurs de ces entreprises, peu importe où ces grappes se trouvent sur la planète. L'entreprise est tenue de donner suite à leur demande d'accès et ne peut informer la personne ou l'institution concernée de la consultation de ses renseignements par le gouvernement américain. Des modifications apportées dernièrement à la *Patriot Act* et à d'autres lois (en vertu de la *USA Freedom Act*) ont réduit les pouvoirs les plus visibles de la NSA, mais la loi (y compris divers décrets-lois) autorise encore les fonctionnaires américains à demander aux fournisseurs de services de leur communiquer des documents, informatiques ou autres, sur des personnes, à leur insu. Même si elles avaient connaissance d'une demande d'accès, les personnes visées qui n'ont pas la citoyenneté américaine pourraient difficilement la contester devant les tribunaux américains ayant compétence pour statuer sur les litiges découlant de la *Patriot Act*, parce qu'ils ne jouissent pas des mêmes droits et protections que les citoyens américains. Ces personnes ne bénéficient pas non plus des protections minimales accordées en vertu de cette loi et d'autres lois sur la surveillance*.

La surveillance par un gouvernement du travail du personnel académique est une violation fondamentale de la liberté académique. Étant donné le cadre légal qui régit les activités de surveillance du gouvernement des États-Unis, les données sur le corps professoral hébergées chez un fournisseur de services infonuagiques de ce pays sont automatiquement plus vulnérables que si elles étaient

---

* Le 26 août 2015, une décision arbitrale a été rendue relativement à un grief opposant le Nova Scotia Government and General Employees Union (NSGEU) et l'Université Dalhousie. Le NSGEU contestait la décision de l'Université de passer avec Microsoft Inc. un contrat en vue de la fourniture d'un système de courrier électronique et d'outils collaboratifs en vertu duquel les renseignements personnels des employés seraient stockés à l'extérieur du Canada, en dérogation de la *Personal Information International Disclosure Protection Act* (PIIDPA) de la Nouvelle-Écosse. L'arbitre a rejeté le grief, estimant que, en l'espèce, l'externalisation des données ne contrevenait pas à la PIIDPA. Les arguments présentés ont uniquement porté sur la question de savoir s'il y avait violation ou non de la PIIDPA et l'arbitre n'a pas tenu compte des clauses des conventions collectives du personnel académique sur la liberté académique ou la protection de la vie privée. Cependant, l'ACPPU juge préoccupantes les conclusions de l'arbitre, car en autorisant l'Université à passer un contrat avec une entreprise dont le serveur est basé aux États-Unis et dont les centres de données sont disséminés dans le monde entier, il a privé les syndiqués du droit de regard sur leurs renseignements personnels.

stockées dans un système interne de l'établissement d'enseignement. Il est vrai que le gouvernement canadien a resserré dernièrement sa politique de surveillance, mais les renseignements stockés dans les centres de données de fournisseurs de services infonuagiques basés au Canada demeurent plus à l'abri de la surveillance – malgré, nous le répétons, l'adoption des lois récentes – que s'ils étaient hébergés dans un centre de données américain.

Les données conservées dans des centres externes peuvent être plus susceptibles d'être violées que celles qui sont sauvegardées sur des serveurs internes, pour plusieurs raisons.

Le nuage n'est pas exempt de piratage, comme l'a démontré le scandale entourant le piratage de comptes d'utilisateurs d'iPhone (des pirates ont accédé à des photos personnelles de célébrités et les ont publiées). Le stockage infonuagique présente d'autres risques : il est notamment plus vulnérable à la communication de données par inadvertance à la suite de pratiques courantes. Cela peut se produire, par exemple, lorsque des employés entrent dans le système de leur employeur à partir d'applications mobiles personnelles non sécurisées. Par ailleurs, en raison de la popularité phénoménale du stockage infonuagique, le déclenchement d'une opération malveillante visant un client peut faciliter l'accès à d'autres clients du même service.

Que peut faire une association de personnel académique? Avoir accès au contrat!

Dès que l'administration d'un établissement envisage de migrer vers l'infonuagique, l'association de personnel académique devrait, avant toute chose, se mobiliser pour obtenir le contrat que l'administration est en train de négocier avec le fournisseur. Le contrat comportera des clauses cruciales sur le niveau de sécurité (p. ex. si les données sont chiffrées ou non pendant leur stockage ou leur transmission) et le niveau d'accès du fournisseur aux données concernant le personnel académique (p. ex. si le fournisseur peut ou non explorer les données pour les vendre à des entreprises de marketing). De plus, le contrat énoncera les conditions d'utilisation que les utilisateurs finaux, le personnel académique en l'occurrence, seront contraints d'accepter pour avoir accès aux services externalisés (stockage des données, communications électroniques ou autres), ou y fera référence.

De nombreuses administrations justifieront leur répugnance à donner accès au contrat par l'obligation de protéger la vie privée ou l'avantage concurrentiel du fournisseur. Les associations de personnel académique devraient être prêtes à prendre des engagements raisonnables à préserver la confidentialité du contenu du contrat si c'est le prix à payer pour y avoir accès.

En raison de la place grandissante qu'occupent les ordinateurs et diverses ressources électroniques dans l'exercice de la profession, le contenu des clauses contractuelles est une des premières lignes de défense de la liberté académique. Tout se joue vraiment dans les détails; il faut donc absolument pouvoir prendre connaissance du contrat pour donner une protection absolue aux données et aux communications du corps professoral.

Une fois leur accès au contrat assuré, les associations de personnel académique devraient porter une attention particulière aux quelques exemples ci-dessous de failles relevées dans plusieurs contrats.

Sécurité des données

Le contrat doit indiquer précisément la norme de sécurité à respecter, plutôt qu'un simple engagement à se conformer à la norme en vigueur dans l'industrie ou à des normes applicables à des informations semblables. Le contrat doit aussi prescrire le chiffrage des données (stockage et transmission) et rendre obligatoire l'envoi rapide d'un avis de violation des données, le cas échéant.

Accès du fournisseur aux données

L'exploration des données doit être interdite à toutes fins, y compris pour la création de tout genre de profil d'utilisateur final. Les exigences en matière de confidentialité des données doivent correspondre aux normes relatives à l'intégrité des recherches des trois conseils subventionnaires. Cependant, il ne suffit pas

d'interdire l'exploration des données; il faut également limiter l'accès du fournisseur aux données du corps professoral aux seules fins de la maintenance des systèmes (p. ex. protéger les systèmes contre les logiciels malveillants ou les pourriels).

Emplacement des données

Il faut interdire le stockage des données en sol étranger. Les grappes de serveurs doivent être situées au Canada pour assurer que les communications échappent à la surveillance de la NSA, une telle surveillance pouvant d'ailleurs constituer une non-conformité à l'obligation de respecter la confidentialité des données de recherche sensibles inscrite dans les normes des trois conseils ou d'autres normes en matière de recherche.

Priorité du contrat conclu entre l'établissement et le fournisseur

De nombreux contrats contiennent une référence à un document externe (comme la politique de confidentialité de Google), qui peut l'emporter sur le contrat passé entre l'établissement et le fournisseur et également être modifié ultérieurement sans que les clients ou les utilisateurs en soient informés. Par exemple, le contrat entre l'établissement et le fournisseur peut interdire l'exploration des données, mais non la politique de confidentialité en vigueur ou future de Google.

Propriété des données

Le contrat doit préciser que les droits de propriété intellectuelle reviennent à l'établissement (et aux utilisateurs).

Modifications au contrat

Le contrat doit indiquer que les modifications au contrat doivent être approuvées par toutes les parties. Il ne faut jamais accepter une clause qui confère au fournisseur le droit de modifier unilatéralement les conditions du contrat.

Ressort et lois applicables

Le contrat doit spécifier que le ressort compétent pour régler les litiges est celui dans lequel se trouve l'établissement.