



Commissariat
à la protection de
la vie privée du Canada

Visez les nuages :

*Questions liées à la protection de la vie
privée dans le contexte de l'informatique
dans les nuages*

Mars 2010

Table des matières

Sommaire.....	1
Examen du concept de l’informatique dans les nuages	2
Qu’est-ce que l’informatique dans les nuages?.....	2
Aperçu de l’informatique dans les nuages	2
Problèmes généraux liés à l’informatique dans les nuages.....	3
Apparente neutralité au chapitre des compétences	4
Absence de contrôle des utilisateurs.....	4
Consentement valable compromis.....	4
Détournement d’usage.....	4
Ralentissement de l’innovation	5
Risques d’atteinte à la vie privée associés à l’informatique dans les nuages.....	5
Compétences	5
Création de nouveaux flux de données	5
Sécurité	6
Atteinte à la sécurité des données	6
Accès légal.....	6
Traitement	7
Mauvaise utilisation des données	7
Permanence des données.....	7
Propriété des données.....	7
Champ de compétences du commissariat à la protection de la vie privée	8
Traitement	8
Relation en nuage directe.....	8
Compétences propres au Commissariat.....	9
Accusearch.....	9
Jurisprudence canadienne relative à la compétence	10
Les règles de base	10
Morguard	10
Beals.....	11
Compétence sur Internet.....	11
Disney.....	12
Intermix.....	13
Conclusion.....	14

Sommaire

L'informatique dans les nuages est une expression générale utilisée pour décrire une sorte d'infrastructure émergente. Elle s'applique à tout système qui permet de stocker de l'information ou une application en ligne et auquel les utilisateurs ont accès par l'entremise d'un dispositif. Aux fins de cette application ou de ces données, l'ordinateur personnel devient essentiellement un « terminal non intelligent », soit une machine qui interagit avec un ordinateur central dans les nuages pour le stockage, l'extraction ou la manipulation de données.

De façon générale, le modèle d'informatique dans les nuages soulève des inquiétudes relativement à ce qui suit :

- apparence de neutralité au chapitre des compétences;
- absence de contrôle des consommateurs;
- consentement valable concernant la publicité;
- détournement d'usage;
- ralentissement de l'innovation.

L'infrastructure dans les nuages pose également des difficultés propres à la vie privée :

- Compétences
- Création de nouvelles données
- Sécurité
- Atteintes à la sécurité des données
- Accès autorisé
- Traitement
- Mauvaise utilisation des données
- Permanence des données
- Propriété des données

Dans le cas où la commissaire à la protection de la vie privée a la compétence sur l'objet d'une plainte mais où la plainte porte sur une infrastructure d'informatique dans les nuages qui n'est pas localisée de façon évidente au Canada, la jurisprudence actuelle est sans équivoque : la commissaire à la protection de la vie privée peut exercer sa compétence quand elle juge qu'il existe un lien réel et substantiel avec le Canada.

L'existence d'un tel lien doit être établie en fonction d'une flexibilité fondée sur des principes et, bien que la jurisprudence établisse un certain nombre de facteurs susceptibles d'entrer en ligne de compte à cet égard, la liste de ces facteurs n'est pas exhaustive et aucun de ces facteurs n'est déterminant en soi — il est par conséquent évident que l'évaluation doit être faite au cas par cas, compte tenu du contexte général dans lequel la plainte a été déposée.

Examen du concept de l'informatique dans les nuages

Qu'est-ce que l'informatique dans les nuages?

De nos jours, l'expression « informatique dans les nuages » semble omniprésente. On la retrouve dans les reportages des médias, dans les publications d'affaires et dans les publications technologiques. En même temps, cette expression est si nébuleuse que de nombreux consommateurs ne sont peut-être pas pleinement conscients de ce qu'elle signifie en réalité.

Un sondage de Pew Internet réalisé en 2008 définissait l'informatique dans les nuages comme une infrastructure émergente selon laquelle les données et les applications résident dans le cyberspace, ce qui permet aux utilisateurs d'y accéder à partir de n'importe quel dispositif connecté au Web¹. L'informatique dans les nuages est notamment utilisée pour des activités courantes comme le stockage de photos en ligne (sur des sites comme flickr); le stockage de vidéos en ligne (sur des sites comme YouTube); l'utilisation d'applications en ligne comme la suite Google Office, Facebook ou Twitter; l'utilisation de services de courrier électronique comme Gmail ou hotmail; le paiement pour le stockage de fichiers électroniques en ligne ou même la création de fichiers de sauvegarde en ligne au moyen de services comme Jungle Disk. Le sondage de Pew Internet portait sur ces six activités et montre que 69 % des utilisateurs en ligne interrogés avaient effectué au moins l'une de ces activités². Des chiffres aussi élevés donnent à penser que l'informatique dans les nuages n'est pas tant la « voie de l'avenir » qu'une technologie déjà de plus en plus répandue.

Jonathan Zittrain inclut ce qu'il appelle les « appareils tenus en laisse » dans l'informatique dans les nuages, tout en signalant que l'utilisation de ces dispositifs peut être particulièrement insidieuse puisque le code et les données peuvent bien demeurer près de l'utilisateur de sorte que ces dispositifs ne donnent pas l'impression d'être des appareils d'informatique dans les nuages, alors qu'ils le sont en réalité, l'utilisateur ayant renoncé à sa liberté de contrôler son code et ses données³. Parmi ces dispositifs tenus en laisse, il y aurait l'omniprésent iPhone ainsi que les appareils de lecture comme le Kindle d'Amazon.

Peu importe la manière dont l'informatique dans les nuages est utilisée, on peut dire qu'elle a pour effet de nous ramener à l'époque des ordinateurs centraux et des terminaux qui ont marqué les débuts de l'informatique — c'est-à-dire que l'ordinateur personnel devient essentiellement un « ordinateur non intelligent », soit une machine qui interagit avec un ordinateur central dans les nuages pour stocker, extraire ou manipuler des données.

Aperçu de l'informatique dans les nuages

Un examen de la documentation donne à penser que l'informatique dans les nuages a une valeur évidente pour les utilisateurs. Les infrastructures d'informatique dans les nuages n'assurent-elles pas un accès

¹ John B. Horrigan (septembre 2008) « Data Memo : Use of cloud computing Applications and Services ». Pew Internet and American Life Project à http://www.pewinternet.org/~media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf [Pew Internet]

² Pew Internet à 1

³ Jonathan Zittrain (30 juillet 2009) « Ma'am, the cloud is coming from inside your house » Future of the Internet (and how to stop it) Blog. [Zitflux Blog]

immédiat aux ressources en « matériel » sans nécessiter d'investissement de capitaux? Ne permettent-elles pas de lancer les projets sur le marché plus rapidement étant donné qu'ils ne requièrent pas de mise au point technique, de même que d'imputer la TI aux coûts opérationnels et de faciliter l'étalement des opérations⁴? Comme le fait valoir Cory Doctorow, l'infrastructure de l'informatique dans les nuages permet aux entreprises qui offrent des services d'accéder à un espace de stockage et d'hébergement illimité, et à celles qui exploitent des superordinateurs de puiser dans la grille informatique de haute performance existante plutôt que de tenter de la reproduire⁵.

Pourtant, il semble qu'il y ait aussi un certain nombre d'inconvénients à l'informatique dans les nuages. On pose comme hypothèse que ses infrastructures sont fondées sur un modèle de fonctionnement selon lequel l'utilisateur paiera en permanence pour quelque chose qu'il obtient actuellement à forfait, voire gratuitement. Or, l'informatique dans les nuages suppose un accès réseau et on peut dire que cet accès est plus lent, qu'il coûte plus cher et qu'il est moins fiable que celui assuré par les disques durs ou les « unités centrales » (UC), et enfin que son utilisation est susceptible d'être interdite, surveillée ou modifiée par des forces externes comme le gouvernement, les employeurs ou les organismes d'exécution de la loi⁶. Et puis, bien sûr, même si les utilisateurs paient pour ces services, ils n'ont pas ou on ne leur accorde pas « le savoir expert ni le contrôle quant à l'infrastructure technologique qui fournit ces services⁷ » [traduction]. Devant de tels inconvénients, on peut s'étonner que l'informatique dans les nuages connaisse un tel succès, mais le sondage de Pew Internet indique que la convivialité et la souplesse expliquent la faveur dont elle jouit actuellement. Selon ce sondage, 51 % des utilisateurs mentionnent la facilité et la convivialité d'utilisation; 41 % d'entre eux apprécient la souplesse qui leur permet de n'être pas captifs d'un site ou d'un dispositif; et 39 % disent aimer la facilité que procure l'informatique dans les nuages au chapitre du partage des données⁸.

Il semble que l'informatique dans les nuages engloberait donc fondamentalement tous les systèmes qui stockent de l'information ou des applications en ligne et qui assurent un accès à cette information ou à ces applications à partir de n'importe quel dispositif. Cette définition délibérément générale permet diverses situations d'« informatique dans les nuages » — un utilisateur qui interagit avec une application dans les nuages; une entreprise qui crée une infrastructure dans les nuages privée qu'elle utilise dans son propre environnement; ou même une organisation (en ligne ou non) qui choisit d'utiliser cette infrastructure pour le stockage ou le traitement de ses données.

Problèmes généraux liés à l'informatique dans les nuages

Une fois que nous avons compris ce qu'est l'informatique dans les nuages, un certain nombre de problèmes généralisés deviennent évidents.

⁴ Bandyopadhyay, Subhajyoti, Marston, Sean R, Zhang, Juheng, Li, Zhi et Ghalsasi, Anand, « Cloud computing: The Business Perspective » (3 juin 2009). Disponible à SSRN : <http://ssrn.com/abstract=1413545> à 7 [The Business Perspective]

⁵ Cory Doctorow (2 septembre 2009) « Not Every Cloud Has a Silver Lining ». The Guardian. <http://www.guardian.co.uk/technology/2009/sep/02/cory-doctorow-cloud-computing>

⁶ Doctorow

⁷ The Business Perspective à 7

⁸ Pew Internet à 2

Apparente neutralité au chapitre des compétences

Premièrement, il y a ce que Picker appelle la « neutralité de l'informatique dans les nuages » [traduction] — c'est-à-dire l'« hypothèse implicite [...] que le fait de changer l'emplacement du traitement ou du stockage des données ne change rien quant à la façon dont le flux des données traitées ou stockées est utilisé⁹ » [traduction]. Évidemment, cela pourrait ne pas être le cas et causer des problèmes tant pour les organisations qui choisissent de conclure un contrat avec des fournisseurs d'infrastructure dans les nuages que pour les fournisseurs eux-mêmes, de même que compromettre la sécurité des données et, par le fait même, la sécurité des personnes.

Absence de contrôle des utilisateurs

Les événements récents qui ont entouré le Kindle indiquent également qu'il y a des problèmes inhérents au modèle d'informatique dans les nuages, surtout en ce qui a trait aux appareils tenus en laisse¹⁰. Qu'il s'agisse de la décision d'Amazon de retirer de leurs bibliothèques Kindle sans le consentement des consommateurs des exemplaires d'un certain roman qu'ils ont déjà achetés, de la fermeture des sites de GDN et donc de l'interdiction d'accès des consommateurs à de la musique qu'ils ont déjà payée ou même du pouvoir implicite que confèrent des stratégies comme le processus d'« approbation » d'Apple pour les applications iPhone et des implications de censure qui en découlent, il est manifeste que le fait de laisser ce pouvoir entre les mains du fournisseur d'un site peut entraîner et entraîne effectivement des problèmes imprévus et des risques pour les consommateurs.

Consentement valable compromis

Le modèle lui-même crée également des problèmes en ce sens que s'il devient le modèle d'utilisation des ordinateurs par défaut, les entreprises ne pourront plus se financer elles-mêmes par la vente de copies de leurs logiciels. Cette éventualité pose un risque : l'abandon de la vente de contenu entraînera forcément une dépendance à l'égard du modèle gratuit, financé par la publicité¹¹. Même si ce modèle ne présente pas de problème inhérent, on peut croire (à juste titre) qu'il existe un problème quand il n'y a plus de solutions de rechange et que le choix et le consentement éclairés sont moins possibles.

Détournement d'usage

Le modèle d'informatique dans les nuages peut également inciter les entreprises à accroître leur taille ou élargir leur champ d'activité ou la portée de leur consentement afin de tirer profit de l'information qu'elles recueillent.¹²

⁹ Randal C. Picker (2009) « Competition and Privacy in Web 2.0 and the Cloud ». John M. Olin Law & Economics Working Paper N° 414 (2^e série). Université de Chicago à 7[Competition and Privacy]

¹⁰ Jonathan Zittrain (20 juillet 2009) « Lost in the Cloud ». Article figurant en regard de la page éditoriale, *New York Times*, 20 juillet 2009 [Zittrain NYT]

¹¹ Randal C. Picker (2009) « Online Advertising, Identity and Privacy » John M. Olin Law & Economics Working Paper n° 475 (2^e série) Université de Chicago

¹² Competition and Privacy à 13

Ralentissement de l'innovation

En ce qui concerne la concurrence et l'innovation, le modèle d'informatique dans les nuages soulève des inquiétudes. Les critiques ont dénoncé le caractère spécifique d'un site éventuellement créé ou mis sur pied dans le contexte de rapports commerciaux avec une entité particulière dans les nuages¹³. Par exemple, certaines organisations comptent sur l'information accumulée au cours de longues périodes pour optimiser l'efficacité de leurs plateformes — cet investissement en temps, combiné aux modalités d'utilisation qui interdisent d'exporter les données vers d'autres sites, soulève des problèmes doubles, la capacité des utilisateurs de changer de fournisseur étant restreinte alors que l'innovation et la création d'autres plateformes offrant des services analogues sont également limitées parce que les utilisateurs sont moins susceptibles de vouloir ou pouvoir passer d'une plateforme à l'autre.

Risques d'atteinte à la vie privée associés à l'informatique dans les nuages

Le fait que l'informatique dans les nuages crée une distance entre les personnes et leurs données soulève des problèmes de protection de la vie privée et d'application des pouvoirs de réglementation inhérents au modèle.

Compétences

De par sa nature, l'informatique dans les nuages permet de transmettre, de stocker et de traiter des données à divers endroits. Selon les lois et les méthodes de protection des données, cela peut provoquer des problèmes au chapitre des compétences¹⁴. D'ailleurs, la prépondérance du modèle d'informatique dans les nuages pourrait même remettre en question la notion de « propriété » des données, sur laquelle repose une bonne partie du système de protection des données, ce qui conduirait plutôt à des analyses fondées sur l'authentification des données¹⁵.

Création de nouveaux flux de données

Le modèle d'informatique dans les nuages pourrait entraîner la création d'énormes fonds de (nouvelles) données et les mettre à la disposition de l'infomédiaire-fournisseur de services d'informatique dans les nuages. Quand l'infomédiaire a la capacité de voir ce qui se passe à chaque clic, il peut produire un riche flux de données¹⁶. Même si ce flux de données pourrait être sans rapport avec les opérations dans les nuages originales, il risque d'être utilisé soit par l'organisation soit par l'infomédiaire dans les nuages à des fins qui vont au-delà de celles pour lesquelles le consentement avait été donné au départ. Le sondage de Pew Internet a démontré que les utilisateurs s'inquiètent vivement que leurs données soient (mal) utilisées dans l'environnement de l'informatique dans les nuages (90 % d'entre eux craignent que leurs données soient vendues à une autre organisation; 80 % se disent préoccupés de ce que leurs photos ou autres données soient utilisées dans des campagnes de marketing; et 68 % affirment qu'ils seraient inquiets si leurs données étaient analysées et utilisées à des fins de publicité ciblée)¹⁷.

¹³ Competition and Privacy à 9

¹⁴ The Business Perspective à 9

¹⁵ The Business Perspective à 14

¹⁶ Competition and Privacy à 5

¹⁷ Pew Internet à 2

Sécurité

Par définition, l'informatique dans les nuages suppose un partage/transfert d'information sur Internet. Cela soulève des questions de sécurité en ce qui concerne la protection des flux de données et les mesures de sauvegarde et de sécurité appliquées aux données pendant qu'elles résident dans l'environnement de l'informatique dans les nuages.

Christopher Soghoian a soulevé des questions quant à la sécurité des transactions de l'informatique dans les nuages et a fait valoir que les fournisseurs de services d'informatique dans les nuages ont eu tendance à délaissier les solutions éprouvées en matière de sécurité¹⁸. Pour appuyer ses arguments, il souligne que les fournisseurs de services d'informatique dans les nuages pourraient (et devraient) à tout le moins utiliser les moyens courants de cryptage utilisés par les banques et les détaillants en ligne pour protéger leurs flux de données, mais que la plupart ne le font pas actuellement. Quant à la sécurité de l'entreposage, comme l'indique Doctorow, si les applications de l'informatique dans les nuages étaient conçues de manière à défendre les intérêts des utilisateurs plutôt que d'accroître l'efficacité des modèles opérationnels, les données seraient massivement cryptées¹⁹.

Atteinte à la sécurité des données

On a vu plus haut que les utilisateurs renoncent à un certain niveau de contrôle lorsqu'ils sont en interaction avec une infrastructure d'informatique dans les nuages. On connaît un certain nombre d'interactions de ce genre — les fournisseurs de services d'informatique dans les nuages ou les applications dans les nuages, qui peuvent avoir accès aux données qu'ils détiennent, les exploiter ou les transformer en marchandises; les pouvoirs exercés par le secteur public ou le secteur privé, qui permettent la gestion ou la fermeture de sites ou de discours particuliers; ou de simples acteurs du secteur privé qui ne peuvent résister à la fascination qu'exercent les bases de données qui s'offrent à eux. Dans tous les cas, non seulement les données d'une personne sont à risque dans l'infrastructure d'informatique dans les nuages, mais il est possible que cette personne ne prenne jamais conscience de l'atteinte.

Accès légal

Au-delà du risque généralisé d'intrusion gouvernementale, l'informatique dans les nuages soulève des préoccupations particulières quant à l'accès légal aux données. L'accès légal en soi est bien sûr préoccupant, que l'information soit stockée dans l'ordinateur de l'utilisateur, chez un fournisseur de services Internet ou auprès d'un fournisseur de services d'informatique dans les nuages. Toutefois, l'utilisation de l'infrastructure d'informatique dans les nuages comporte des risques supplémentaires.

Par exemple, dans le cas où plusieurs entreprises utilisent une infrastructure d'informatique dans les nuages centralisée, une demande d'accès légal auprès du fournisseur de services d'informatique dans les nuages peut permettre de recueillir de l'information de toutes les autres entreprises. D'autre part, si les données personnelles et les données du FSI sont stockées ensemble dans un environnement d'informatique dans les nuages, une demande d'accès légal peut donner accès à une information plus élaborée que celle que prévoit

¹⁸ Christopher Soghoian (2009) « Caught in the Cloud: Privacy, Encryption and Government Back Doors in the Web 2.0 Era ». SSRN

¹⁹ Doctorow

la législation sur l'accès légal. Enfin, comme dans le cas des autres formes d'intrusion, la distance qui existe entre les données et leur propriétaire dans l'environnement de l'informatique dans les nuages accroît la possibilité non seulement que les intéressés ne soient pas conscients qu'il existe un accès légal à leurs données mais que le fournisseur de services lui-même n'en soit pas conscient.

Traitement

Une organisation qui envisage de recourir au service de stockage ou de traitement de ses données dans l'infrastructure d'informatique dans les nuages d'un tiers est censée « impartir le traitement » de ses données et doit donc examiner les questions de protection des renseignements (tant en ce qui concerne l'intrusion que la sauvegarde et la récupération des données) et contraindre le fournisseur de l'informatique dans les nuages à des contrôles en matière de protection de la vie privée égaux à ceux imposés à l'organisation responsable des données, et doit faire en sorte que des procédures d'accès et de correction soient en vigueur, et que les procédures de suppression soient adéquates.

Mauvaise utilisation des données

Il est particulièrement important de définir les paramètres du rapport entre le traitement ou le stockage des données, étant donné la possibilité (examinée ci-dessus) que le fournisseur d'une infrastructure d'informatique dans les nuages accède de façon abusive aux données qui lui sont confiées par une organisation et les manipule ou les exploite également de façon abusive. Le cas échéant, les organismes de réglementation devront pouvoir distinguer entre les gestes du fournisseur de services d'informatique dans les nuages *en tant que responsable du traitement* et ceux qui dépassent la relation de traitement et qui, par conséquent, attireront directement l'attention de l'organisme de réglementation.

Permanence des données

Un autre risque important de l'informatique dans les nuages concerne la permanence des données. Outre les conditions des contrats destinées à faire en sorte que les données soient protégées pendant qu'elles sont en la possession d'un fournisseur de services d'informatique dans les nuages, il est important de tenir compte de l'utilisation que l'on fera des données. Il faudra prendre des mesures pour veiller à ce que toutes les copies des données soient retirées définitivement de l'infrastructure d'informatique dans les nuages, et régir dans quel délai ces copies seront retirées.

Propriété des données

Par ailleurs, la création de nouveaux flux de données pourrait susciter des inquiétudes quant à leur propriété. Bien que la propriété des données confiées à une infrastructure d'informatique dans les nuages aux fins de stockage semble assez explicite, la propriété des données téléchargées vers une infrastructure d'informatique dans les nuages risque d'être moins certaine. Enfin, il y a les données secondaires générées par suite des interactions avec une infrastructure d'informatique dans les nuages — même s'il s'agit de « renseignements personnels identifiables » en vertu de la LPRPDE, il se peut que les utilisateurs ne soient pas informés de la création ou de l'existence de ces données.

Champ de compétences du commissariat à la protection de la vie privée

La commissaire à la protection de la vie privée du Canada a pour mandat de superviser la conformité tant à la *Loi sur la protection des renseignements personnels*²⁰ (LPRP) qu'à la *Loi sur la protection des renseignements personnels et les documents électroniques*²¹ (LPRPDE). La LPRP régleme les pratiques de gestion de l'information des organismes du gouvernement du Canada, tandis que la LPRPDE utilise les pouvoirs en matière de commerce du gouvernement fédéral pour établir des attributions relatives à la collecte, à l'utilisation et à la communication de renseignements personnels par des organisations du secteur privé dans le cadre d'activités commerciales.

Selon toute vraisemblance, une plainte traitant d'informatique dans les nuages relèverait de la LPRPDE; il est également possible que le gouvernement du Canada crée une infrastructure de « nuage privé » à l'interne pour faciliter l'échange d'information ou bien que certaines institutions gouvernementales, ou l'ensemble de celles-ci, utilisent une infrastructure en nuage pour traiter ou stocker les données.

Traitement

Si une organisation a transféré des données à un fournisseur de services d'infrastructure dans les nuages, il est probable qu'en vertu de la LPRPDE, de telles actions soient perçues comme étant un transfert à des fins de traitement; par conséquent, selon le principe 4.1.3 de l'annexe 1, l'organisation devrait s'assurer qu'un niveau de protection comparable est fourni pour l'information. L'organisation continuerait de contrôler l'information et d'être responsable de la conformité avec les exigences de la LPRPDE. Le Commissariat a déjà fait enquête sur des plaintes de cette nature par le passé et l'a fait de manière efficace. Il a aussi communiqué des lignes directrices sur le traitement transfrontalier des données personnelles²².

Relation en nuage directe

Il est important de souligner que le transfert de renseignements à un tiers fournisseur de services d'infrastructure dans les nuages à des fins de traitement n'est pas le seul moyen que peut prendre le Commissariat pour intervenir. Par exemple, une organisation (publique ou privée) pourrait créer un « nuage privé » à l'interne pour faciliter l'échange de renseignements entre différents endroits ou différentes parties de l'organisation. D'autre part, une personne pourrait interagir directement avec un fournisseur de services d'infrastructure dans les nuages, que ce soit en utilisant ses services pour du stockage ou en accédant à des applications en nuage et en les utilisant. Finalement, il y a toujours la possibilité que l'information confiée à un fournisseur de services d'infrastructure dans les nuages puisse être accédée, utilisée, exploitée ou autrement marchandée sans obtention du consentement par le fournisseur de services d'infrastructure dans les nuages. Dans chacune de ces situations, les dispositions de la loi pertinente (LPRPDE ou LPRP) s'appliqueraient à l'objet d'une telle plainte.

²⁰ L.R.C. 1985, chap. P-21

²¹ L.C. 2000, chap. 5

²² Lignes directrices sur le traitement transfrontalier des données personnelles
(http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.asp)

Compétences propres au Commissariat

Accusearch

L'affaire *Lawson c. Accusearch Inc.*²³ consistait en une demande de révision judiciaire dans laquelle la compétence du Commissariat était directement visée.

Dans cette affaire, une personne a tenté de déposer une plainte auprès du Commissariat contre Accusearch Inc., une entreprise américaine qui fournit des services de recherches sur des données de base, de profils psychologiques, de traces de courriels, de registres des appels, etc. La personne alléguait qu'Accusearch recueillait, utilisait et communiquait des renseignements personnels sur les Canadiens à des fins inappropriées à l'insu des personnes concernées et sans le consentement de celles-ci, ce qui contrevient à la LPRPDE.

Sur réception de la plainte, la commissaire à la protection de la vie privée a examiné le dossier de façon préliminaire et a conclu qu'elle ne pouvait accepter la plainte puisque l'enquête nécessiterait l'exercice de ses pouvoirs de manière extraterritoriale, ce qui dépasse les limites de ses compétences telles qu'elles sont décrites dans la LPRPDE.

Le juge Harrington était d'avis que la décision de la commissaire de ne pas accepter la plainte était erronée; il a indiqué que « la commissaire n'a pas bien fait la différence entre son pouvoir de mener enquête et l'efficacité de son enquête²⁴ ». Il a établi des analogies en comparant la situation à celle dans *SOCAN*²⁵, où la Cour suprême du Canada a rapporté qu'il existe un lien suffisant pour l'attribution de la compétence quand le Canada est soit le pays de transmission ou de réception et a par conséquent découvert que, même si la commissaire avait raison d'affirmer que le Parlement n'avait aucunement l'intention de légiférer extraterritorialement et ne l'a effectivement pas fait, la LPRPDE pouvait néanmoins s'appliquer si le différend présentait un lien suffisant avec le Canada pour justifier l'exercice de compétences canadiennes²⁶.

La Cour a conclu en stipulant que la commissaire à la protection de la vie privée a compétence pour mener enquête sur des plaintes portant sur la circulation transfrontalière de renseignements personnels²⁷. Cette conclusion était principalement fondée sur une analyse qui démontrait que la commissaire était compétente à l'égard de l'objet de la plainte (la collecte, l'utilisation et la communication de renseignements personnels) et de la personne pour autant qu'un lien réel et substantiel est mis en évidence entre l'entité ou les faits reprochés et le Canada. Le juge a aussi tenu compte du pouvoir relatif à l'endroit, mais a indiqué que le fait qu'une enquête pouvait s'avérer infructueuse en raison de l'incapacité de la commissaire à assigner à comparaître ou à autrement forcer des organisations à collaborer à son enquête ne constituait pas un motif suffisant pour refuser de prendre la plainte. Par conséquent, la Cour fédérale a accepté la demande de révision judiciaire et a adressé de nouveau la plainte au Commissariat.

La décision *Accusearch* établit alors que, même si une entreprise ou un site Web se trouve à l'extérieur du territoire canadien, si la commissaire à la protection de la vie privée du Canada a compétence sur l'objet d'une

²³ [2007] 4 R.C.F. 314.

²⁴ *Accusearch*, par. 27.

²⁵ *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, [2004] 2 R.C.S., 427.

²⁶ *Accusearch*, par. 26-29.

²⁷ *Accusearch*, par. 51.

plainte et peut établir un lien réel et substantiel avec le Canada, elle peut exercer sa compétence à l'égard de la plainte.

Jurisprudence canadienne relative à la compétence

Les règles de base

Morguard

En ce qui a trait à la question de la compétence, l'affaire canadienne à l'origine est *Morguard Investments Ltd. c. De Savoye*²⁸, qui portait sur la compétence entre les provinces canadiennes. Cette affaire visait à établir si les tribunaux d'une province (Colombie-Britannique) devaient reconnaître et faire appliquer un jugement prononcé par les tribunaux d'une autre province (Alberta) si le défendeur ne réside pas dans la province du tribunal qui rend la décision au moment du procès.

La décision de la Cour suprême du Canada débute avec l'interprétation suivante : « les règles du droit international privé sont fondées sur la nécessité qu'impose l'époque moderne de faciliter la circulation ordonnée et équitable des richesses, des techniques et des personnes d'un pays à l'autre »²⁹ et part de ce point pour essayer d'aborder le problème en tenant compte de cette circulation d'un pays à l'autre. Pour en venir à cette décision, le juge La Forest a pris en considération de nombreux facteurs; il a étudié les jurisprudences anglaise et canadienne, des travaux universitaires, l'importance de la Constitution canadienne pour établir une vision unifiée entre sphères de compétence du Canada³⁰ et la question connexe de la structure judiciaire du Canada menant à la Cour suprême du Canada pour ainsi s'assurer qu'il n'existe pas de différence de qualité de justice entre les provinces³¹. Il conclut en énonçant que « les règles de la courtoisie et du droit international privé doivent, dans leur application entre les provinces, respecter la structure fédérale de la Constitution³² ».

Par conséquent, la Cour a établi dans cette affaire que « les tribunaux d'une province devraient reconnaître totalement les jugements rendus par un tribunal d'une autre province ou territoire, pourvu que ce tribunal ait correctement et convenablement exercé sa compétence dans l'action³³ ». En vue de déterminer si la compétence a été exercée correctement et convenablement, le juge La Forest a utilisé le critère visant à déterminer s'il existe « un lien réel et substantiel entre le ressort et l'acte dommageable³⁴ ».

À l'aide de ce critère, la Cour suprême du Canada a déterminé que l'action contre De Savoye avait été intentée convenablement en Alberta. Dans les faits, étant donné que les propriétés se trouvaient en Alberta, que les contrats ont été conclus en Alberta par des parties qui résidaient alors en Alberta et que l'action en forclusion

²⁸ [1990] 3 R.C.S. 1077.

²⁹ Morguard, 22.

³⁰ Morguard, 25.

³¹ Morguard, 25.

³² Morguard, 26.

³³ Morguard, 28.

³⁴ Morguard, 31. Ce critère est fondé sur la décision du juge Dickson dans *Moran c. Pyle National (Canada) Ltd* [1975] 1 R.C.S. 393.

a eu lieu en Alberta, le juge La Forest était d'avis que l'« on peut difficilement imaginer un lien plus réel et substantiel entre le préjudice subi et le ressort³⁵ ».

L'affaire Morguard établit donc le critère de base pour l'exercice approprié de la compétence — la présence d'un lien réel et substantiel entre le préjudice subi et la compétence.

Beals

Évidemment, l'affaire Morguard traitait de la compétence entre les provinces, mais toujours à l'intérieur du Canada. Ce n'est qu'avec l'affaire *Beals c. Saldanha*³⁶ que l'application de cette approche pour des jugements prononcés par des tribunaux à l'extérieur du Canada a été approuvée. Alors que certains tribunaux provinciaux avaient déjà élargi le critère de Morguard pour l'appliquer à de telles situations³⁷, la Cour suprême du Canada en tenait compte pour la première fois.

En se fondant sur la décision rendue dans l'affaire Morguard, le juge Major a conclu que :

La courtoisie internationale et la prédominance de la circulation et des opérations transfrontalières internationales commandent une modernisation du droit international privé. L'application des principes énoncés dans l'arrêt *Morguard* et analysés davantage dans l'arrêt *Hunt*³⁸ peut et doit déborder le cadre de la reconnaissance des jugements d'une autre province, même si elle peut faire intervenir d'autres considérations sur le plan international. À moins que les législatures n'adoptent des lois prescrivant une approche différente, le critère du « lien réel et substantiel » devrait également s'appliquer à la reconnaissance et à l'exécution des jugements étrangers³⁹.

Par conséquent, l'arrêt *Beals* vient élargir le critère de Morguard sur le « lien réel et substantiel » aux décisions rendues à l'extérieur du pays.

Compétence sur Internet

Au Canada, deux affaires récentes mettent en évidence l'application du critère de « lien réel et substantiel » à des entités en ligne.

³⁵ Morguard, 33.

³⁶ [2003] 3 R.C.S. 416.

³⁷ Voir *Moses c. Shore Boat Builders Ltd.* (1993), 106 D.L.R. (4th) 654 (C.A.C.-B.), autorisation de pourvoi refusée, [1994] 1 R.C.S. xi; *United States of America c. Ivey* (1996), 30 O.R. (3d) 370 (C.A.); *Old North State Brewing Co. c. Newlands Services Inc.*, [1999] 4 W.W.R. 573 (C.A.C.-B.).

³⁸ *Hunt c. T&N plc*, [1993] 4 R.C.S. 289. Cet arrêt portait sur une loi du Québec qui interdit le retrait du Québec de tout document concernant une entreprise commerciale au Québec. Cette loi était utilisée pour empêcher une action en justice en Colombie-Britannique; la Cour suprême du Canada a par la suite établi que la présence de telles lois d'obstruction allait au-delà des pouvoirs de la province étant donné que leur essence touchait des sujets à l'extérieur de la province du Québec.

³⁹ *Beals*, par. 28.

Disney

L'affaire *Disney Enterprises Inc. v Click Enterprises Inc.*⁴⁰ traite d'une situation opposant Disney à différents sites Web enregistrés au nom de Click Enterprises. Les sites Web étaient enregistrés au moyen d'une adresse à Toronto (Ontario) et l'entreprise est enregistrée en tant que société ontarienne. Ces sites Web vendaient des adhésions fournissant aux clients des outils et de la technologie pour les aider à télécharger des films (protégés par le droit d'auteur) et offrant du soutien en ligne aux abonnés qui avaient de la difficulté à repérer ou à télécharger des films qu'ils recherchaient. Disney a intenté une poursuite devant un tribunal de New York et a obtenu un jugement totalisant 486 442,17 \$. La décision de la Cour supérieure de justice de l'Ontario cherchait à déterminer si la Cour de New York a exercé convenablement sa compétence de manière à ce que la Cour de l'Ontario puisse appliquer le jugement de New York.

La juge Lax était d'avis que la jurisprudence existante établissait que « la détermination de l'exercice adéquat de sa compétence par un tribunal dépend de deux principes : le besoin d'ordre et de justice et l'existence d'un lien réel et substantiel avec soit la cause d'action ou le défendeur⁴¹ » [traduction] .

Quand les parties au litige sont rattachées à de multiples territoires de compétence, la juge Lax estime que l'exigence relative à l'ordre et à la justice est respectée s'il existe des motifs raisonnables d'exercer la compétence. Dans la présente affaire, la juge Lax a noté que Disney est une société du Delaware, exploitée principalement à partir de la Californie, mais qui distribue des films partout aux États-Unis et ailleurs dans le monde. D'autre part, Click Enterprises appartenait à des résidents de l'Ontario qui avaient enregistré l'entreprise en Ontario; toutefois, l'entreprise comprenait des sites Web interactifs par l'intermédiaire desquels des ententes d'abonnement étaient vendues à des résidents des États-Unis, y compris à des résidents de New York. Étant donné que, au Canada, il est établi par la loi que le lien nécessaire pour entendre une cause est suffisant si le Canada est soit le pays de transmission ou de réception⁴², la juge Lax a conclu qu'il existait effectivement des motifs raisonnables pour que la Cour de New York accepte la cause; l'exigence relative à l'ordre et à la justice a donc été respectée.

Au moment de déterminer s'il existait un lien raisonnable et substantiel entre New York et la cause, la juge Lax a examiné à fond la jurisprudence existante avant d'évaluer les faits de l'affaire en question et d'établir ce qui suit :

Dans la présente affaire, Click Enterprises, pour atteindre ses fins commerciales, a utilisé Internet pour pénétrer les États-Unis et mener à bien ses activités. L'entreprise a signé des contrats avec des fournisseurs de services de paiement aux États-Unis pour traiter des paiements par Internet sur ses sites Web. Au début, Click a signé un contrat avec une société canadienne; quand VISA a modifié sa réglementation, elle s'est constituée en personne morale sous le nom Click Enterprises Inc. (Delaware) pour que les paiements passent par cette société⁴³. [traduction]

Après avoir conclu qu'il existait un lien raisonnable et substantiel, la juge Lax a poussé son examen encore plus loin et s'est penchée sur les arguments qui avaient été invoqués par Click Enterprises voulant que les services étaient offerts à l'échelle mondiale, et non seulement aux États-Unis ou à New York, que New York était un

⁴⁰ (2006) 267 D.L.R. (4th) 291 (Ont. S.C.J.).

⁴¹ Disney, par. 11.

⁴² *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Assoc. canadienne des fournisseurs Internet*, [2004] 2 R.C.S., 427 à 457.

⁴³ Disney, par. 22.

« territoire de compétence choisi au hasard » et que l'on n'avait pas répondu au critère de lien réel et substantiel. Dans sa réponse, la juge Lax a fait remarquer que Click Enterprises savait qu'elle avait des clients américains, que, dans les faits, la plupart des « témoignages » sur ses sites Web provenaient d'Américains et que « quand les activités sont menées sur Internet, elles peuvent causer des préjudices n'importe où et partout. Les sites Web des défendeurs étaient mis à la disposition des résidents de New York par l'entremise des canaux de distribution habituels, et c'est à cet endroit qu'ils ont causé des préjudices⁴⁴ » [traduction]. Elle suppose cependant que, si Disney avait profité d'un quelconque avantage juridique en raison de la compétence juridictionnelle, la Cour aurait pu étudier la question plus en détail, mais, dans les circonstances, elle était convaincue que New York « était non seulement un territoire de compétence adéquat pour intenter la poursuite, mais aussi un territoire qui est, pourrait-on dire, plus juste pour les défendeurs que si la poursuite avait été intentée, comme cela aurait pu se produire, dans un territoire de compétence géographiquement plus éloigné, comme la Californie⁴⁵ » [traduction].

Après avoir tenu compte des moyens de défense soulevés, la juge Lax a conclu que la Cour de New York avait convenablement exercé sa compétence à l'égard de l'affaire; par conséquent, rien n'empêchait les tribunaux de l'Ontario d'appliquer le jugement rendu dans l'État de New York.

Intermix

L'autre décision récente, qui date aussi de 2006, est l'affaire *Desjean c. Intermix Media Inc.*⁴⁶. Dans cette affaire, Patrick Desjean a déposé un recours collectif envisagé contre Media dans lequel il alléguait que l'entreprise avait contrevenu à la *Loi sur la concurrence* en fournissant des logiciels espions/logiciels publicitaires avec ses logiciels gratuits sans le faire savoir à ses clients qui obtenaient les logiciels gratuits. Intermix s'est vue signifier l'action et a répondu au moyen d'une demande d'ordonnance rejetant la demande de M. Desjean en invoquant le fait que la Cour fédérale du Canada n'avait pas compétence⁴⁷.

Même si Intermix contestait l'allégation voulant qu'elle ait tout de même distribué des logiciels espions ou qu'elle ait omis d'aviser les clients des logiciels publicitaires fournis avec certains programmes, la constatation de la Cour fédérale n'était pas fondée sur cet élément.

Le juge DeMontigny a déterminé que le critère de compétence adéquat était le critère du lien réel et substantiel, conformément à ce qui est établi dans l'affaire *Morguard*. Il a noté ce qui suit : les serveurs d'Intermix ne se trouvaient pas au Canada et le fait de subir des dommages sur un ordinateur au Canada n'est pas suffisant pour établir un lien; Intermix n'a pas de bureaux au Canada et n'a jamais conservé ni loué de locaux à bureaux au Canada; Intermix n'a pas d'employés au Canada bien que l'entreprise ait une relation contractuelle avec deux entrepreneurs indépendants au Canada qui fournissent des services sans lien avec la présente affaire; Intermix ne s'est prévalue d'aucune loi canadienne; Intermix n'a pas de comptes bancaires canadiens, ne verse pas d'impôts canadiens, n'est pas enregistrée aux fins de la TPS ni de la TVP et n'est enregistrée en tant qu'entreprise nulle part au Canada; Intermix ne fait pas de publicité, de sollicitation ni de commercialisation au Canada, n'a jamais pris part à des salons professionnels ou autres événements

⁴⁴ Disney, par. 29.

⁴⁵ Disney, par. 29.

⁴⁶ (2006) C.F. 1395.

⁴⁷ Dans les faits, les représentants invoquaient soit : (a) que la Cour fédérale n'avait pas compétence à l'égard d'Intermix et de la question; (b) que la demande de M. Desjean était frivole et vexatoire; (c) que la demande de M. Desjean constituait un abus de procédure.

promotionnels au Canada; dans les faits, il serait manifestement injuste d'assujettir Intermix à la compétence d'un tribunal canadien puisque cela signifierait qu'une entreprise ne possédant pas de biens d'entreprise au Canada et n'étant pas physiquement présente dans le territoire de compétence pourrait faire l'objet d'une poursuite dans n'importe quel pays dans lequel ses produits sont téléchargés. Par conséquent, le juge a déterminé qu'« étant donné que le critère de l'existence d'un lien minimal entre le défendeur et le ressort en question doit nécessairement être plus rigoureux lorsqu'un autre pays est en jeu (par opposition à un autre État fédéré du même pays), je me vois dans l'impossibilité de conclure qu'Intermix a un lien minimal avec le Canada ou avec l'objet de la présente action ».

La décision de la Cour fédérale a été contestée en 2007⁴⁸, mais l'appel a été rejeté.

Conclusion

La commissaire à la protection de la vie privée du Canada a pour tâche de superviser la conformité tant avec la *Loi sur la protection des renseignements personnels*⁴⁹ (LPRP) qu'avec la *Loi sur la protection des renseignements personnels et les documents électroniques*⁵⁰ (LPRPDE). Selon toute vraisemblance, une plainte traitant d'informatique dans les nuages relèverait de la LPRPDE; toutefois, il est également possible que le gouvernement du Canada crée une infrastructure de « nuage privé » à l'interne pour faciliter l'échange d'information ou bien même que certaines institutions gouvernementales, ou l'ensemble de celles-ci, utilisent une infrastructure en nuage pour traiter ou stocker les données.

L'informatique dans les nuages est une expression générale définissant une nouvelle sorte d'infrastructure. En termes simples, il s'agit de tout système qui stocke de l'information et/ou des applications en ligne, de manière à permettre à l'utilisateur d'y accéder à partir de n'importe quel dispositif.

La nature de l'informatique dans les nuages semble, à première vue, créer des tensions possibles entre les organismes de protection des données/des renseignements personnels, les FSI et les clients en raison de l'incertitude quant à l'identité de l'organisation qui devrait être responsable dans le cas d'atteintes à la vie privée et à la façon de tenir responsables, en vertu de la loi canadienne, les entreprises qui se trouvent « dans les nuages ».

Les plaintes que le Commissariat recevrait sur l'informatique dans les nuages découleraient probablement de l'une des quatre situations suivantes :

- une organisation qui choisit d'utiliser l'infrastructure en nuage pour l'entreposage et/ou le traitement des données;
- une organisation ou un organisme gouvernemental qui crée une infrastructure de nuage privé pour faciliter l'échange de renseignements dans ses environs;
- un utilisateur individuel qui interagit avec une application en nuage;
- l'utilisation abusive des données par un fournisseur d'infrastructure en nuage à qui les données ont été fournies.

⁴⁸ (2007) CAF 365.

⁴⁹ L.R.C. 1985, ch. P-21.

⁵⁰ L.C. 2000, ch. 5.

Dans le premier cas, il est probable que, en vertu de la LPRPDE, de telles actions soient perçues comme étant un transfert à des fins de traitement; par conséquent, selon le principe 4.1.3 de l'annexe 1, l'organisation devrait s'assurer qu'un niveau de protection comparable est fourni pour l'information. L'organisation continuerait de contrôler l'information et d'être responsable de la conformité avec les exigences de la LPRPDE. Le Commissariat a déjà fait enquête sur des plaintes de cette nature par le passé et l'a fait de manière efficace. Il a aussi communiqué des lignes directrices sur le traitement transfrontalier des données.

Pour les deuxième, troisième et quatrième situations, les dispositions de la loi pertinente (LPRPDE ou LPRP) s'appliqueraient à l'objet d'une telle plainte.

Quand la commissaire a compétence à l'égard de l'objet de la plainte, mais que la plainte traite d'une infrastructure informatique dans les nuages (et qu'il n'est donc pas évident d'établir qu'elle se situe au Canada), la jurisprudence existante énonce clairement que la commissaire peut exercer sa compétence si l'évaluation indique un lien réel et substantiel avec le Canada.

La jurisprudence stipule que la compétence peut être exercée à l'égard d'entités extraterritoriales quand il est possible d'établir un lien réel et substantiel avec le territoire de compétence. Cela a été le cas à la fois pour des questions de compétence interprovinciale et internationale, bien qu'un lien plus strict puisse être exigé dans des contextes internationaux. Le critère du lien réel et substantiel doit être abordé sous l'angle d'une flexibilité réglée par des principes; bien que la jurisprudence établisse un certain nombre de facteurs pouvant être pris en compte pour faire une telle évaluation, la liste n'est pas exhaustive et aucun des facteurs n'est en soi déterminant — l'évaluation du lien doit plutôt être réalisée au cas par cas.