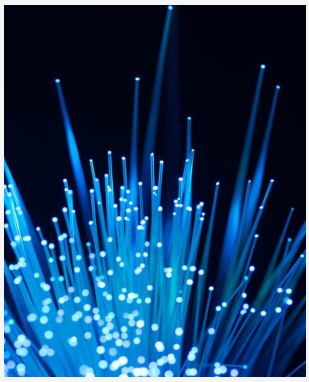
OSLER

La souveraineté des données au regard du CLOUD Act : retour vers le futur?

7 OCTOBRE 2025 18 MIN DE LECTURE



Expertises Connexes

- Respect de la vie privée et gestion de l'information
- Technologie

Auteurs(trice): Michael Fekete, John Salloum

Ottawa et les gouvernements provinciaux partout au pays sont confrontés à des demandes voulant que les données des Canadiens soient protégées, en partie, contre l'accès obtenu depuis l'étranger en vertu de la loi américaine connue sous le nom de *CLOUD Act*. Ces demandes sont devenues plus insistantes à la suite des récentes évolutions politiques bilatérales et de la réémergence d'une question très médiatisée, celle de la « souveraineté des données », c'est-à-dire la garantie que les tribunaux canadiens sont les seuls tribunaux à avoir un pouvoir sur les données stockées au Canada. Certains commentateurs expriment également des inquiétudes quant à la sécurité des données stockées auprès de fournisseurs de services infonuagiques américains. De plus, l'adoption de solutions de « nuage souverain » fait l'objet de discussions de plus en plus fréquentes à tous les niveaux du gouvernement.

Ces discussions ont lieu à un moment où :

- il n'existe aucun cas documenté où un gouvernement ou des forces de l'ordre d'un pays étranger auraient eu accès à des données d'entreprises canadiennes traitées par des fournisseurs de services infonuagiques;
- les idées fausses sur le *CLOUD Act* sont courantes (par exemple, le *CLOUD Act* ne crée pas de pouvoirs de surveillance ni d'accès illimité aux documents stockés par des fournisseurs de services infonuagiques ou d'autres services numériques au Canada);
- le recours à un fournisseur de services canadien ou le stockage de données au Canada ne garantit pas que les données seront hors de portée des tribunaux d'autres pays;
- la Colombie-Britannique a mis fin à une tentative importante visant à imposer la souveraineté des données;
- il est de plus en plus évident que, à l'ère du numérique, pour gérer les renseignements de manière efficace, il faut recourir à une approche fondée sur les risques qui tient compte de tous les coûts et facteurs pertinents, y compris la disponibilité de solutions technologiques.

Dans le présent bulletin, nous explorons la prévalence de l'accès obtenu depuis l'étranger aux dossiers électroniques stockés au Canada, les répercussions du *CLOUD Act* et les diverses stratégies d'atténuation des risques perçus qui y sont liés.

La prévalence des communications de contenus de clients d'entreprises stockés hors des États-Unis est très faible

Les principaux fournisseurs de services infonuagiques publient régulièrement des rapports de transparence destinés à informer le public sur le nombre et les types de demandes de communication de données utilisateur qu'ils reçoivent des gouvernements et des tribunaux du monde entier, y compris des États-Unis. Bien que, de façon générale, ces rapports ne mentionnent pas les demandes de communication de données stockées au Canada, les chiffres montrent clairement que, à l'échelle mondiale, la prévalence des communications de contenus de clients d'entreprises stockés hors des États-Unis est très faible.

Qu'est-ce que le *CLOUD Act*?

La loi intitulée *Clarifying Lawful Overseas Use of Data Act* (le *CLOUD Act*) a été promulguée par le Congrès américain en 2018 afin de moderniser les lois relatives aux demandes légitimes de renseignements à l'ère de l'informatique en nuage.

Le *CLOUD Act* n'a pas créé de *nouveaux* pouvoirs permettant aux forces de l'ordre des États-Unis d'obtenir des données. Il a plutôt appliqué les règles traditionnelles aux fournisseurs de services de communication électronique ou de services infonuagiques relevant de la compétence des tribunaux américains, y compris les entreprises étrangères faisant affaire aux États-Unis. Ce faisant, le *CLOUD Act* a précisé que ces fournisseurs de services étaient tenus de se conformer aux mandats visant des renseignements stockés hors des États-Unis si les renseignements en question étaient sous leur garde ou leur contrôle ou en leur possession, tout en maintenant les protections de courtoisie prévues par la common law. En d'autres termes, les fournisseurs peuvent contester les demandes de communication de données produites par les forces de l'ordre des États-Unis en vertu du *CLOUD Act* si cela enfreint les lois de leur pays.

En outre, le *CLOUD Act* a autorisé les gouvernements des États-Unis et de pays étrangers à négocier des accords bilatéraux réciproques permettant aux forces de l'ordre des deux pays de soumettre leurs demandes de renseignements transfrontalières directement aux fournisseurs de services, ce qui permet de réduire les délais autrement associés aux traités d'entraide judiciaire (TEJ), lesquels peuvent s'étirer sur des mois, voire des années. Le Canada et les États-Unis travaillent sur un tel accord depuis 2022, mais les négociations, qui ont été engagées à la suite du Forum sur la criminalité transfrontalière, une initiative favorisant la collaboration dans la lutte contre la cybercriminalité, l'extrémisme violent et la violence armée, n'ont toujours pas abouti à ce jour.

Ces pouvoirs ne sont pas nouveaux

Bien que certains commentateurs aient cité le *CLOUD Act* comme un exemple d'ingérence extraterritoriale de la part des États-Unis, de nombreux autres pays disposent d'outils juridiques permettant à leurs forces de l'ordre enquêtant sur des crimes graves d'accéder à des données électroniques stockées à l'étranger. Au Canada, des sociétés étrangères ayant une présence virtuelle au pays ont été contraintes de produire des données stockées à l'étranger dans le cadre d'une enquête criminelle[1]. Au Royaume-Uni, la loi intitulée *Crime (Overseas Production Orders) Act* donne aux forces de l'ordre locales un mécanisme leur permettant d'obtenir des données électroniques stockées à l'étranger. Dans l'Union européenne, le Règlement concernant les preuves électroniques prévoit un processus similaire par lequel le tribunal d'un État membre peut ordonner à un fournisseur de services infonuagiques d'un autre État membre de produire ou de conserver des preuves

électroniques, quel que soit le lieu où les données sont stockées.

Toutes ces lois, y compris le *CLOUD Act*, ont en commun le fait qu'elles concernent les enquêtes criminelles relevant de la compétence des tribunaux locaux. En d'autres termes, elles ne donnent pas aux forces de l'ordre ou aux gouvernements étrangers un accès illimité aux renseignements traités par les fournisseurs de services. Elles facilitent plutôt la collecte limitée de données dans le cadre d'enquêtes criminelles lorsque le fournisseur est soumis à la compétence du tribunal.

Idées fausses couramment véhiculées sur le *CLOUD Act*

Idée fausse : Le *CLOUD Act* a créé des pouvoirs de surveillance.

Réalité : Aucun pouvoir de surveillance n'a été créé. Le *CLOUD Act* a clarifié la procédure judiciaire en vigueur aux États-Unis.

Idée fausse : Le *CLOUD Act* permet au gouvernement ou aux forces de l'ordre des États-Unis d'accéder librement aux renseignements traités par les fournisseurs de services infonuagiques au Canada.

Réalité : L'accès aux courriels, documents ou vidéos que les Canadiens créent, communiquent ou stockent à l'aide de services infonuagiques nécessite un mandat autorisé par un tribunal. Un tel mandat nécessite l'établissement d'une cause probable, fondée sur des faits crédibles, d'un acte criminel relevant de la compétence des États-Unis. Les mandats sont limités aux types de données expressément indiqués dans le mandat. La collecte de données en vrac n'est pas autorisée. Les données non liées à du contenu, telles que les données des abonnés, nécessitent une ordonnance d'un tribunal, une assignation à comparaître ou une procédure judiciaire similaire.

Idée fausse : Le *CLOUD Act* permet au gouvernement américain d'accéder aux secrets commerciaux et autres biens de propriété intellectuelle traités par les fournisseurs de services infonuagiques.

Réalité : Le *CLOUD Act* s'applique uniquement aux enquêtes criminelles relevant de la compétence des tribunaux américains. Les secrets commerciaux et autres biens de propriété intellectuelle sont très rarement pertinents dans le cadre d'une enquête criminelle.

Idée fausse : Le *CLOUD Act* oblige les fournisseurs de services infonuagiques à mettre au point un accès détourné aux données stockées qui ont été cryptées.

Réalité : Le *CLOUD Act* n'oblige pas les fournisseurs de services infonuagiques à décrypter les renseignements et ne les empêche pas de proposer à leurs clients des outils de chiffrement ou des outils similaires qui retirent les données de la possession, de la garde ou du contrôle du fournisseur. Elle interdit également l'inclusion d'une obligation de déchiffrement dans tout accord bilatéral conclu aux termes du *CLOUD Act*[2].

Idée fausse : Le *CLOUD Act* repose sur un processus judiciaire secret.

Réalité : Les mandats obtenus en vertu du *CLOUD Act* le sont conformément au processus judiciaire applicable aux affaires pénales, tel qu'il existait aux États-Unis jusqu'alors.

Idée fausse : Le *CLOUD Act* ne prévoit aucun processus de contestation d'un mandat en cas de conflit de lois.

Réalité : Sous le régime du *CLOUD Act*, les contestations fondées sur la « courtoisie » en common law sont toujours possibles[3]. Cela signifie qu'il est possible d'introduire une demande en annulation ou en modification d'un mandat au motif que son exécution serait contraire aux lois d'un autre pays. Le *CLOUD Act* prévoit aussi d'autres motifs de contestation dans les cas où les parties sont dans des pays ayant signé un accord bilatéral.

Idée fausse : Les accords bilatéraux conclus aux termes du *CLOUD Act* compromettent les protections judiciaires.

Réalité : La conclusion d'un accord bilatéral aux termes du *CLOUD Act* dépend de la présence de protections en matière de vie privée, de droits de la personne et d'État de droit[4].

Le stockage de données au Canada ne garantit pas que celles-ci ne seront pas consultées en vertu d'ordonnances de tribunaux étrangers

Les données traitées au Canada par un fournisseur de services étranger ou par un fournisseur de services canadien qui a des activités ou des représentants dans un pays étranger peuvent être soumises à des ordonnances judiciaires hors du Canada. Par exemple, le *CLOUD Act* s'applique à tout fournisseur de services soumis à la compétence des États-Unis[5]. Cela signifie que les forces de l'ordre des États-Unis peuvent signifier une procédure judiciaire à l'entité américaine, la contraignant à produire des données, même si celles-ci sont détenues par une société mère ou une filiale étrangère. La question factuelle que doit examiner un tribunal américain est de savoir si le fournisseur de services aux États-Unis a la « garde, le contrôle ou la possession » (*custody, control, or possession*) des données stockées dans un autre territoire.

Principaux enseignements tirés des précédentes tentatives en matière de souveraineté des données au Canada

À la suite de l'adoption par les Américains de la loi intitulée *Patriot Act* et de l'adoption rapide des services infonuagiques il y a une vingtaine d'années, la souveraineté des données est devenue un sujet de discussion très médiatisé au Canada. À l'époque, les législateurs et les autorités de réglementation ont réagi de façon très variée. En ce qui concerne l'accès aux données et leur localisation, les gouvernements de la Colombie-Britannique et de la Nouvelle-Écosse ont adopté des lois contraignantes régissant la détention et le contrôle de renseignements personnels par les organismes publics. En ce qui concerne les lois sur la protection des renseignements personnels, l'Alberta et le Québec y ont apporté des modifications relativement mineures, mais la plupart des provinces n'y ont apporté aucune modification.

Le Commissariat à la protection de la vie privée du Canada a publié des lignes directrices autorisant le traitement des renseignements personnels à l'étranger à condition que certaines mesures de protection soient en place. Le Conseil du Trésor du Canada a, quant à lui, adopté une approche intermédiaire. Selon sa Directive sur les services et le numérique, les installations informatiques situées à l'intérieur du Canada doivent être considérées en tant qu'« option principale », mais pas la seule, pour la prestation de services impliquant l'information électronique sous le contrôle du gouvernement qui est classée Protégé B, Protégé C ou Classifié.

Peu à peu, la question de la souveraineté des données a perdu de son intérêt, jusqu'à ce que, en 2021, le gouvernement de la Colombie-Britannique modifie sa loi sur la protection des renseignements personnels dans le secteur public dans le but de supprimer les aspects les plus contraignants de ses exigences concernant la localisation des données et leur accès. À l'époque, la Colombie-Britannique avait clairement indiqué qu'elle modifiait ses règles en matière de résidence des données « [traduction libre] afin que les organismes publics puissent utiliser des outils modernes tout en continuant à protéger les renseignements personnels ».

En d'autres termes, la province a essentiellement reconnu que la souveraineté absolue des données n'était pas réalisable dans un monde interconnecté, car elle nuit à la capacité des universités, des écoles, des hôpitaux et des ministères à innover, à gérer leurs coûts et à fonctionner efficacement. En fin de compte, ces exigences sont devenues insoutenables compte tenu de la faible probabilité que les données du secteur public fassent l'objet d'une demande de renseignements de la part d'un gouvernement étranger.

Stratégies d'atténuation des risques liés à la souveraineté des données

Même si le risque est faible, les entreprises canadiennes doivent comprendre ce qu'elles peuvent faire pour atténuer la possibilité que les données dont elles ont la garde ou le contrôle fassent l'objet d'une ordonnance d'un tribunal étranger qui n'est pas soumise à un contrôle judiciaire au Canada.

Recourir à un fournisseur de services canadien

Le recours à un fournisseur de services canadien qui n'a pas d'activités ou de représentants aux États-Unis ou dans un autre pays étranger peut se révéler une stratégie efficace pour l'entreprise qui veut assurer la souveraineté des données, à condition que celles-ci soient stockées et accessibles uniquement au Canada. Toutefois, si le fournisseur de services est présent dans un autre pays, par exemple par le biais de filiales, de bureaux, d'employés, de clients ou d'infrastructures, il peut être soumis à la compétence des tribunaux de ce pays. De plus, comme l'a clairement montré l'expérience du gouvernement de la Colombie-Britannique avec ses règles en matière de résidence des données, avec une telle stratégie, la disponibilité des outils modernes est limitée.

Conserver les données « sur place » au Canada

Comme deuxième stratégie, une entreprise peut traiter ses données exclusivement dans ses propres locaux et derrière son propre pare-feu. Si l'entreprise est détenue et contrôlée au Canada et n'a aucune présence à l'étranger, cette stratégie lui permettra probablement de protéger ses données contre les mandats de tribunaux étrangers. Cependant, pour maintenir une infrastructure sur place, l'entreprise devra engager des capitaux et faire des

investissements importants en matériel, en logiciels, en sécurité et en personnel qualifié, notamment pour soutenir la capacité de sauvegarde et de reprise après sinistre. De plus, les solutions sur place manquent souvent d'évolutivité, de flexibilité et d'accès aux technologies les plus avancées, y compris les cyberdéfenses. Pour ces raisons, les solutions sur place sont de plus en plus réservées au traitement des données les plus délicates, telles que celles qui touchent à la sécurité nationale.

Mettre en place un « nuage souverain »

Un nuage public « entièrement souverain » exigerait que les données soient traitées, transmises et stockées exclusivement au Canada et qu'elles restent toujours sous le contrôle exclusif de fournisseurs de services qui ne sont pas soumis à des lois étrangères autorisant l'accès aux données sans le consentement du client canadien.

La viabilité d'un nuage public « entièrement souverain » est discutable, car il faudrait qu'un tel nuage soit fourni par une entreprise sous contrôle canadien ayant son siège social au Canada et n'ayant pas de présence significative à l'étranger. En réalité, une telle exigence nécessiterait la création et la maintenance d'une solution conçue et fournie au Canada par un fournisseur qui ne dispose pas de l'expérience, de l'expertise et du financement acquis en livrant concurrence sur le marché mondial.

L'expérience récente de l'UE met en évidence les défis liés à la mise en place d'un nuage souverain. En 2019, l'Europe a lancé un projet connu sous le nom de GAIA-X afin de réduire sa dépendance à l'égard des fournisseurs de services infonuagiques étrangers. Six ans plus tard, malgré des investissements de plusieurs milliards d'euros, GAIA-X n'a pas réussi à s'imposer largement sur le marché, et de nombreuses entreprises européennes (sinon la plupart) continuent de s'appuyer principalement sur des fournisseurs de services infonuagiques mondiaux.

Tirer parti des solutions technologiques

La technologie offre une panoplie de solutions permettant de conserver le contrôle des données et d'atténuer, voire d'éliminer, les risques liés à la souveraineté des données. Les solutions technologiques qui sont présentées ci-dessous sont susceptibles de se généraliser au fil des ans, les fournisseurs de services se livrant concurrence pour conquérir et fidéliser les clients soucieux de la souveraineté des données.

- **Chiffrement et gestion des clés :** Chiffrement des données au repos, en transit et en cours d'utilisation. Dans la mesure du possible, les entreprises gèrent leurs propres clés de chiffrement (clés gérées par le client) plutôt que de s'appuyer sur les capacités de chiffrement offertes par le fournisseur de services.
- **Gestion des accès aux données et des identités :** Déploiement de systèmes de gestion des identités et des accès afin de contrôler strictement qui peut accéder aux données et depuis où, avec surveillance et audit des journaux d'accès aux données.
- **Masquage et marquage des données :** Utilisation du masquage ou du marquage des données pour garantir que celles-ci restent illisibles sans interprétation ou déchiffrement local.
- **Informatique confidentielle :** Élimination ou réduction de l'accès aux données pendant leur traitement par la création d'un environnement d'exécution isolé, basé sur du matériel

informatique. Les données traitées dans cet environnement restent invisibles pour le fournisseur de services infonuagiques.

Retour vers le futur?

La réémergence de la souveraineté des données comme enjeu politique au Canada nous invite à réfléchir à la manière dont les gouvernements et les autorités de réglementation partout au pays aborderont cette question dans les mois et les années à venir. La décision du gouvernement de la Colombie-Britannique de modifier sa loi sur la protection des renseignements personnels dans le secteur public en 2021 par la suppression des aspects les plus contraignants de ses exigences concernant la localisation des données et leur accès fournit des « leçons à tirer » qui sont tout aussi pertinentes aujourd'hui, à savoir :

- **Se concentrer sur les risques réels :** Une grande partie du débat public sur la souveraineté des données est motivée par la crainte qu'un gouvernement étranger oblige un fournisseur de services infonuagiques à produire les données d'un client, même si celles-ci sont stockées au Canada. Cependant, rien ne prouve que cela se produise fréquemment.
- **Éviter une approche « taille unique » :** Conformément aux lois sur la protection des données, il faut une approche fondée sur les risques pour assurer la souveraineté des données. À cette fin, il peut être approprié de mettre en œuvre, sur place, des mesures strictes pour les données qui concernent la sécurité nationale ou les opérations militaires, mais, par rapport au niveau de risque, il sera souvent disproportionné d'appliquer ces mesures aux données moins délicates.
- **Tenir compte de tous les coûts sociaux et économiques :** La construction de centres de données au Canada peut être la partie la plus facile de la mise en place d'une solution « souveraine ». La partie la plus difficile – et la plus coûteuse – peut être l'approvisionnement en produits et services souverains qui y seront déployés. De plus, les produits et services souverains sont peu susceptibles d'offrir la même gamme de fonctionnalités améliorant la productivité que les produits et services offerts par le biais du nuage public.
- **Reconnaître les facteurs économiques qui rendent les solutions de nuage souverain difficiles à mettre en œuvre.** La construction de centres de données nationaux ne garantit pas le succès des solutions de nuage souverain. La concurrence avec les fournisseurs de services infonuagiques établis, qui développent leurs technologies depuis des décennies, rend les facteurs économiques du nuage souverain difficiles à mettre en œuvre. De plus, l'acquisition de solutions sur mesure qui ne permettent pas d'exploiter pleinement les infrastructures et les logiciels offerts dans le commerce risque d'augmenter considérablement le coût d'un projet, tout en réduisant l'interopérabilité et la résilience.

---

[1] *R v. Love*, 2022 ABCA 269 (demande d'autorisation d'en appeler devant la Cour suprême du Canada refusée le 20 avril 2023) et *(Re) Service de police de la Ville de Montréal,* 2022 QCCS 3935 (décision de la Cour supérieure du Québec)

[2] *CLOUD Act*, par. 105(a).

[3] *CLOUD Act*, par. 103(c).

[4] Le Département de la justice des États-Unis l'a clairement indiqué dans un livre blanc : « [traduction libre] *Le* CLOUD Act *exige que les accords comprennent de nombreuses dispositions protégeant la vie privée et les libertés civiles. Les ordonnances demandant des données doivent être obtenues légalement en vertu du régime national du pays qui demande les données; elles doivent cibler des personnes ou des comptes précis; elles doivent avoir une justification raisonnable fondée sur des faits articulables et crédibles, la particularité, la légalité et la gravité; et elles doivent être soumises à l'examen ou à la surveillance d'une autorité indépendante, comme un juge ou un magistrat. La collecte de données en vrac n'est pas autorisée*. »

[5] *CLOUD Act*, par. 102(2).