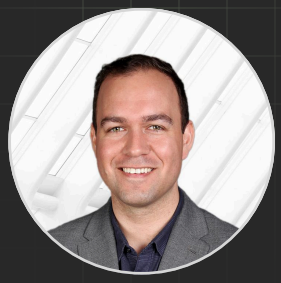
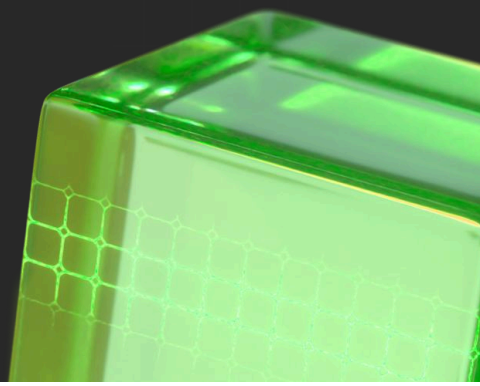
QOHASH



L'adoption de l'IA se fait à la vitesse de la confiance

La sécurité souveraine des données comme pilier essentiel de la stratégie canadienne en IA

Perspectives de Jean Le Bouthillier, PDG et président de Qohash



L'IA redéfinira l'avenir économique et stratégique du Canada. Mais une faille critique est ignorée : **des fournisseurs étrangers dominent la sécurité des données canadiennes.**

L'adoption sécuritaire et souveraine de l'IA au Canada repose sur trois piliers. ① **Des modèles d'IA souverains** comme Cohere pour les usages critiques. ② **Des infrastructures de calcul et d'énergie souveraines** comme l'usine d'IA de TELUS pour opérer à l'échelle nationale. Et ③ **la sécurité souveraine des données** pour protéger les informations sensibles durant tout le cycle de vie de l'IA. Pourtant, ce dernier pilier n'est pas traité comme une priorité dans la stratégie canadienne en IA.

Ce document expose les risques de sécurité des données pour la souveraineté nationale et le contrôle des actifs numériques canadiens, et propose des solutions par l'innovation canadienne en sécurité des données.

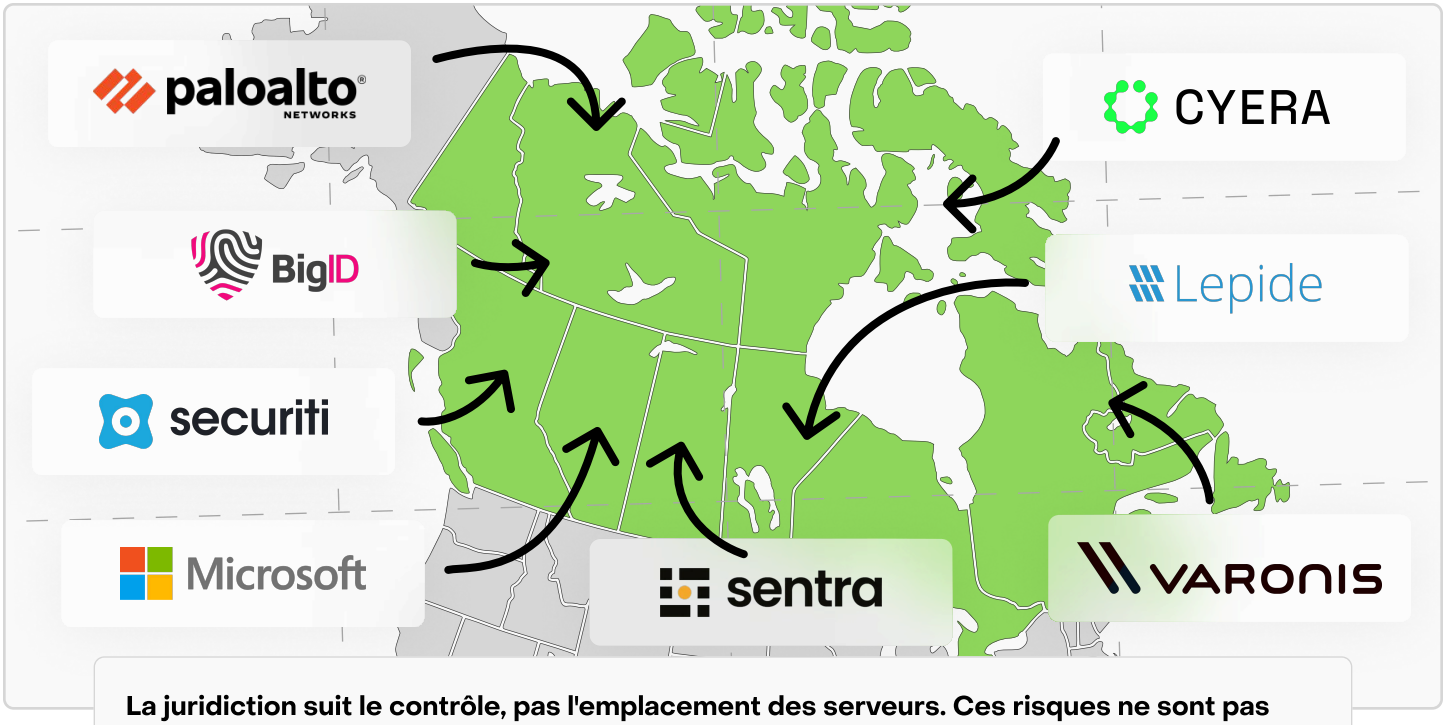
Ce document couvre :

- Domination étrangère en sécurité des données au Canada
- Risques de dépendance aux fournisseurs cloud étrangers
- Qohash, champion canadien de la sécurité souveraine

Qui contrôle la sécurité des données au Canada ?

Le marché canadien de la sécurité des données d'entreprise est massivement dominé par des fournisseurs étrangers. Plusieurs publications du gouvernement du Canada reconnaissent que la dépendance excessive aux fournisseurs cloud et technologiques externes expose les données canadiennes sensibles aux juridictions étrangères, leurs lois, et réduit le contrôle national.[1] [2] [3] Toutefois, ces publications restent politiquement correctes et ne révèlent pas la gravité réelle de la situation sur le terrain :

- La plupart des grandes entreprises et institutions publiques canadiennes dépendent presque entièrement de solutions étrangères de sécurité des données.
- La majorité de ces solutions sont basées dans le cloud, nécessitant la copie de données sensibles vers des environnements tiers pour analyse, augmentant les risques de collecte de renseignements.
- Des fournisseurs basés aux États-Unis et en Israël dominent complètement le marché, contrôlant plateformes, normes, capitaux et distribution.



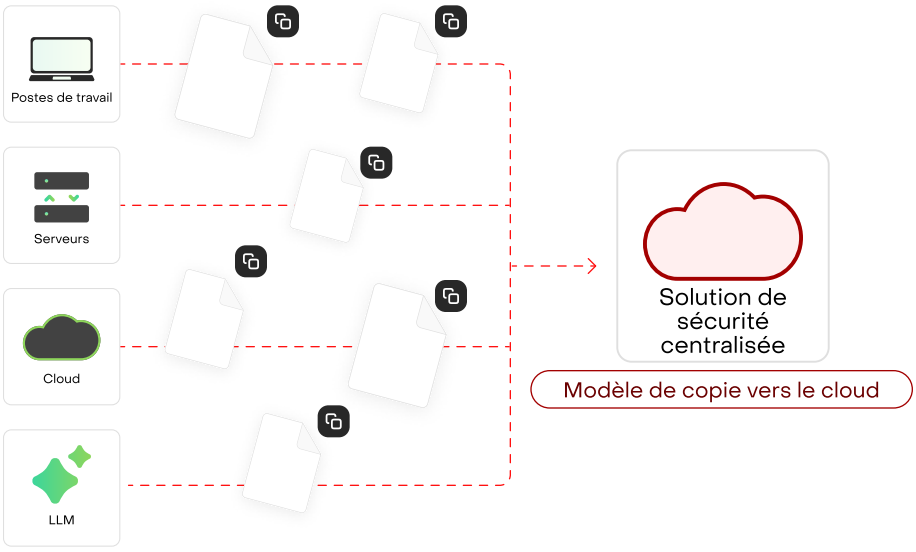
La juridiction suit le contrôle, pas l'emplacement des serveurs. Ces risques ne sont pas théoriques. En 2025, Microsoft a confirmé aux législateurs européens qu'il ne peut garantir la souveraineté des données face à une demande légale américaine, même si les données sont stockées hors des États-Unis.[4] [5] Cette obligation découle du CLOUD Act américain, qui permet aux autorités américaines d'exiger l'accès aux données contrôlées par des entreprises américaines, peu importe leur localisation.[6] Ce cadre juridique s'applique aux données canadiennes détenues sur des plateformes américaines, permettant à une juridiction étrangère de contourner le contrôle canadien.

Quand protéger les données revient à les exposer

La plupart des solutions de sécurité des données utilisées au Canada sont non seulement étrangères, mais aussi basées sur un modèle obsolète et dangereux de centralisation par copie. Ce modèle remonte aux débuts de la sécurité d'entreprise, quand Splunk a été fondé en 2003 et que sécurité signifiait collecter les données dans un système central pour analyse. Avec l'adoption du cloud à la fin des années 2000 et au début des années 2010, des plateformes comme ELK ont étendu cette approche, faisant de la collecte centralisée de données l'architecture par défaut en sécurité, y compris pour la sécurité des données.

La majorité des solutions de sécurité des données copient les fichiers sensibles vers le cloud pour les analyser. Les fichiers des ordinateurs, serveurs, lecteurs partagés et services comme OneDrive sont dupliqués et envoyés à une application tierce. Les contrats promettent une utilisation limitée et la suppression après traitement, mais les données ont quitté l'organisation. Le contrôle est perdu dès la copie. Même avec un cloud canadien, le fournisseur contrôle le logiciel, l'accès et le traitement. Cela crée un risque majeur de collecte de renseignements qui croît à mesure que l'IA accède à des données sensibles à grande échelle.

⚠ Le modèle centralisé de sécurité des données par copie



Quand les outils cloud de sécurité des données sont hébergés au Canada mais opérés par des entreprises étrangères, les données sensibles sont exposées aux obligations légales et stratégiques hors du contrôle canadien.

Pire cas : les données canadiennes sensibles sont exposées à l'accès légal étranger ou la collecte de renseignements.

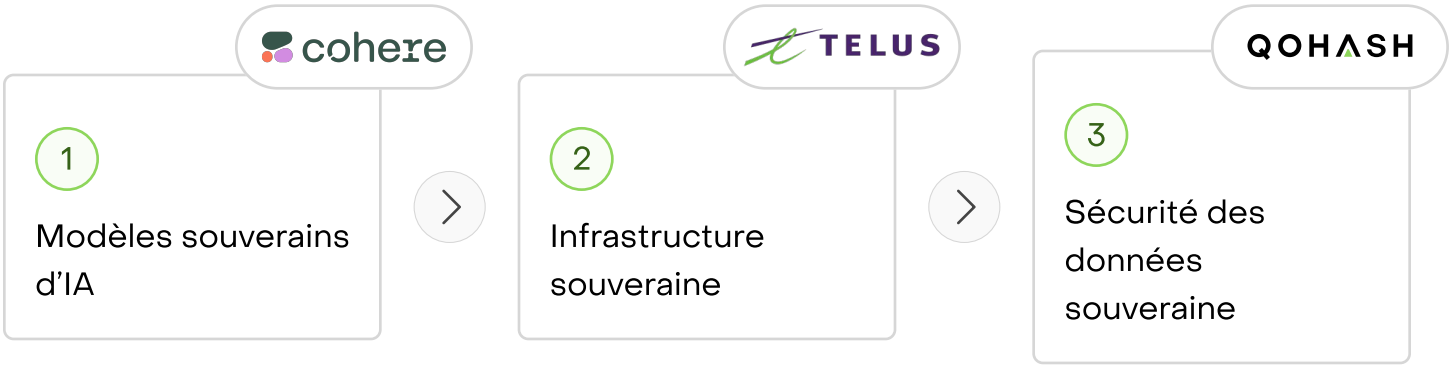
Problèmes majeurs de la sécurité des données cloud par copie

- Les données doivent être copiées vers des plateformes cloud tierces
- Chaque copie augmente l'exposition et la surface d'attaque
- La sécurité s'applique après le déplacement des données
- Les coûts augmentent avec le volume de données analysées et stockées

Adoption sécurisée et souveraine de l'IA

L'adoption sécurisée et souveraine de l'IA au Canada repose sur trois piliers. ① **Des modèles d'IA souverains** comme Cohere pour les usages gouvernementaux, de défense et réglementés. ② **Des infrastructures de calcul et d'énergie souveraines** pour opérer l'IA à l'échelle nationale, comme l'usine d'IA de TELUS. Et ③ **la sécurité souveraine des données** pour protéger les informations sensibles avant, pendant et après l'utilisation de l'IA.

Qohash s'attaque au troisième pilier de sécurité des données, historiquement négligé et sous-financé au Canada. Notre mission est de renforcer la posture de sécurité souveraine des données du Canada pour permettre l'adoption sécuritaire de l'IA sans dépendre de solutions étrangères ni exposer les données sensibles aux risques de collecte de renseignements. Cette mission s'étend aux nations alliées confrontées au même défi. Nous développons aussi une expertise approfondie en cybersécurité et génie logiciel au Canada.



Adoption sécurisée et souveraine de l'IA

Le nom Qohash reflète cette ambition nationale : Q pour Québec, O pour Ontario, où l'entreprise a été conçue. Qohash a été pensée comme entreprise pancanadienne s'étendant de Québec au Grand Toronto. Aujourd'hui, notre ambition et notre empreinte couvrent l'ensemble du Canada, incluant des pôles d'innovation majeurs comme Vancouver, Calgary et Halifax, qui jouent tous un rôle essentiel dans l'émergence du Canada comme fournisseur de solutions de cybersécurité de premier plan.

QOHASH Québec

QOHASH Ontario

QOHASH Hachage de données

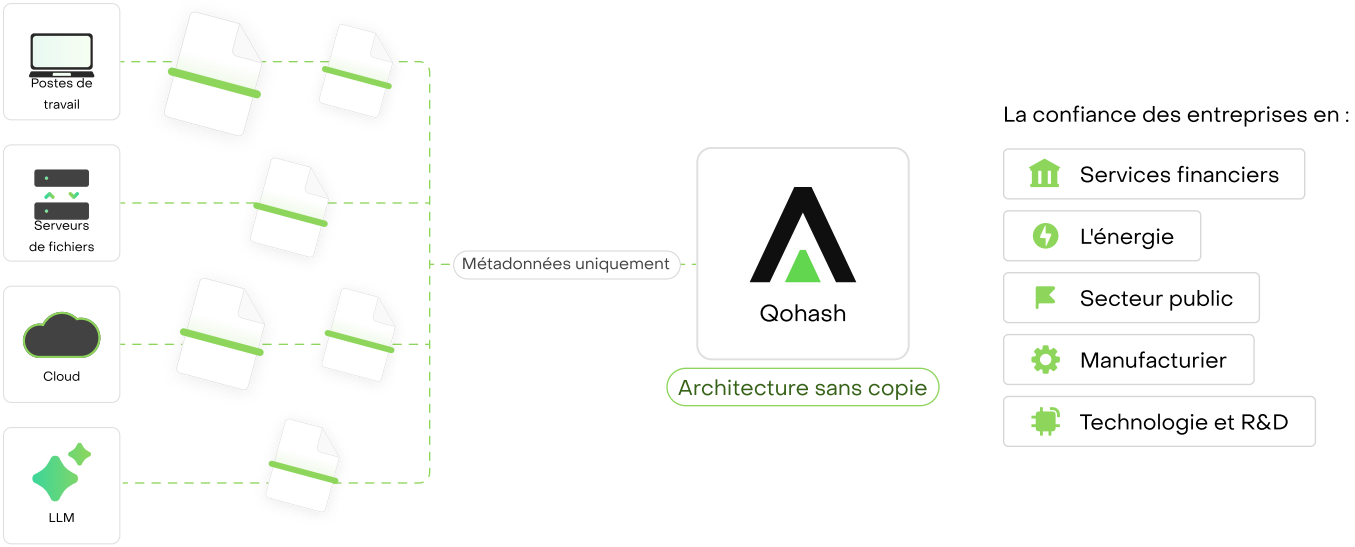
Qohash est un actif national essentiel. Nous développons une technologie de pointe en sécurité des données au Canada — des solutions canadiennes aux problèmes canadiens — que nous exportons pour soutenir l'adoption sécuritaire et souveraine de l'IA mondiale.

Qohash, pionnier de la sécurité des données sans copie

En fondant Qohash, notre objectif était clair : résoudre les problèmes canadiens de sécurité des données avec des solutions canadiennes. Nous nous sommes posé une question simple : **pourquoi envoyer les données sensibles ailleurs pour les analyser ?** Plutôt que de copier et centraliser les données, nous avons conçu le modèle de sécurité des données du futur, fondé sur trois réalités :

- La puissance de calcul augmente de façon prévisible. La loi de Moore demeure fiable, permettant plus de traitement là où les données sont créées.[7]
- Les volumes de données augmentent exponentiellement. La création mondiale de données double environ tous les deux ans, rendant la sécurité centralisée insoutenable.[8]
- L'intelligence se déplace vers la périphérie. L'IA générative et l'analyse avancée sont intégrées directement dans les appareils, serveurs et systèmes locaux, nécessitant une sécurité à la source plutôt que dans des clouds centralisés.[9]

La plateforme de sécurité des données sans copie



L'architecture sans copie élimine le déplacement des données en les sécurisant à la source — la seule approche viable pour des pétaoctets de données non structurées.

- Analyse rapide sur place
- Remédiation native instantanée
- Inventaire complet des données non structurées
- Coûts découplés de la croissance des données

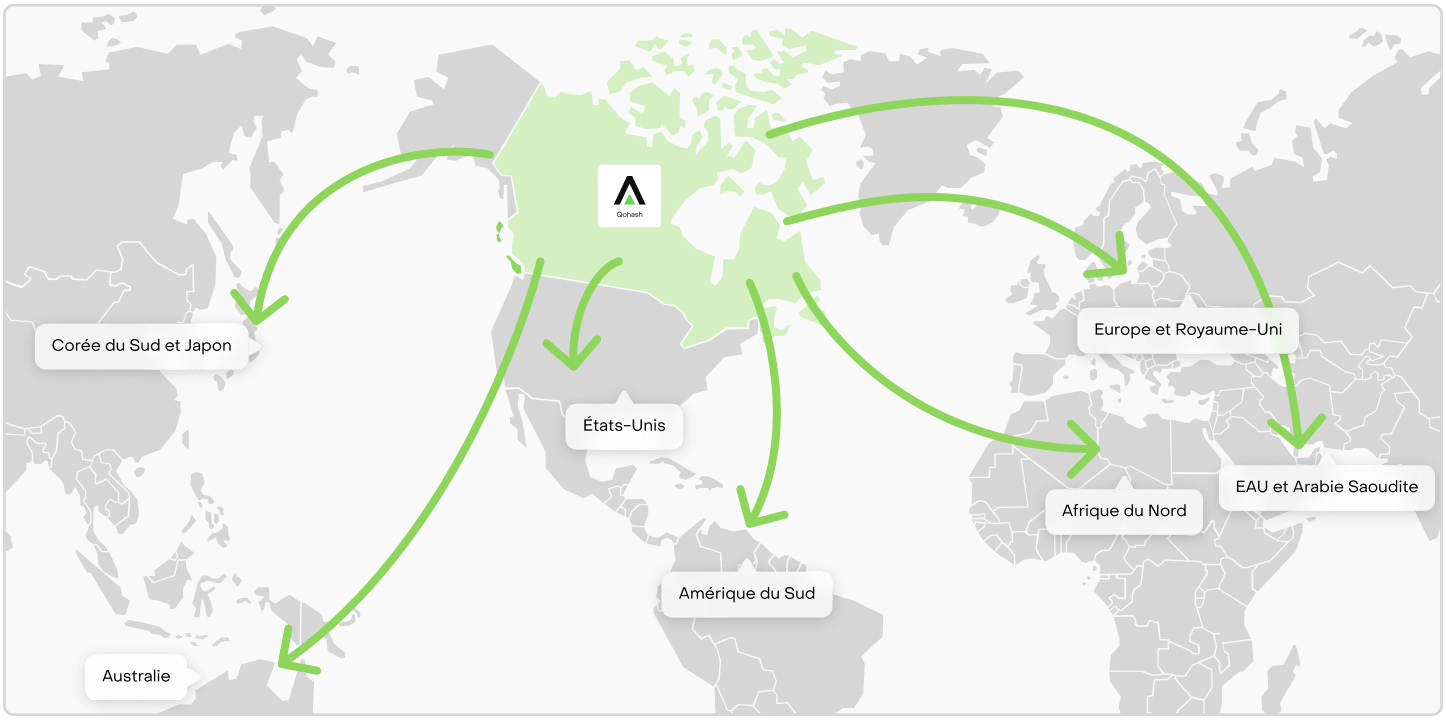
Conçue au Canada, déployée mondialement

Le Canada peut devenir un leader mondial en sécurité des données alors que confiance, souveraineté et contrôle définissent l'ère de l'IA. Avec l'adoption accélérée de l'IA dans les gouvernements, infrastructures critiques, défense et secteur privé, les pays affrontent le même défi : **sécuriser les données sensibles à grande échelle sans céder le contrôle à des plateformes étrangères.**

Qohash vise à faire de la sécurité des données une capacité canadienne déployable mondialement. Fondée sur des principes de base et conçue pour les grandes entreprises, notre approche sans copie répond aux réalités de l'adoption mondiale de l'IA : croissance explosive des données, intelligence croissante à la périphérie, et préoccupations sur la souveraineté et l'exposition juridictionnelle. Ce modèle permet de sécuriser les données là où elles résident, plutôt que de les exporter vers des plateformes centralisées hors de contrôle.

Les gouvernements et entreprises d'Europe, des pays de l'OTAN, du MENA et d'Asie-Pacifique affrontent des défis similaires en réglementation, sécurité et confiance alors que l'IA s'intègre aux opérations quotidiennes. **Le Canada est bien placé pour offrir une alternative crédible et alignée sur ses valeurs, fondée sur la transparence, la confiance et le contrôle souverain.**

C'est une opportunité autant commerciale que stratégique. Exporter les capacités canadiennes en sécurité des données renforce l'influence du Canada dans l'écosystème mondial de l'IA et la résilience nationale.



Le Canada à la tête de la sécurité des données

Notre expérience avec les grandes entreprises et infrastructures critiques révèle ce qu'exige la sécurité des données à l'ère de l'IA.

D'ici 36 mois, le plan de croissance de Qohash générera plusieurs résultats stratégiques pour le Canada :

1 **Développer la disponibilité mondiale depuis le Canada**
Étendre Qohash au-delà du Canada, des États-Unis et de l'Europe vers l'OTAN, le MENA, l'ASEAN et d'autres marchés alliés cherchant des alternatives.

2 **Faire progresser une plateforme sans copie de classe mondiale**
Investir dans le développement pour solidifier le leadership en sécurité des données sans copie comme norme pour l'adoption sécuritaire et souveraine de l'IA.

3 **Bâtir une capacité nationale à double usage**
Renforcer une technologie de sécurité des données utilisable pour l'adoption et la sécurité de l'IA tant commerciale que défensive.

4 **Créer des emplois et une expertise canadienne de haute valeur**
Accroître les effectifs en ingénierie, IA, cybersécurité et commercialisation, créant des emplois technologiques durables et bien rémunérés avec une expertise nationale approfondie.

5 **Ancrer la sécurité des données comme sécurité nationale**
Garantir que la technologie, les opérations et le contrôle restent au Canada, sous gouvernance souveraine et surveillance de confiance.

Qohash est le pionnier de la sécurité des données sans copie, le seul modèle conçu pour sécuriser des pétaoctets de données non structurées dans les grandes entreprises. Qohash mène la transition vers la sécurité autonome des données, identifiant et appliquant continuellement les contrôles de risque à vitesse machine sans déplacer ni copier les données.

Site web : www.qohash.com | Centre de sécurité : trust.qohash.com

AICPA SOC 2 TYPE 2 · AICPA SOC 3 · ISO 27001 · ISO 27701 · ISO 42001

Références

1. Gouvernement du Canada. Livre blanc du gouvernement du Canada : souveraineté des données et nuage public. Secrétariat du Conseil du Trésor du Canada. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html

2. Gouvernement du Canada. Souveraineté numérique dans les environnements en nuage https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html

3. Sécurité publique Canada. Stratégie nationale de cybersécurité du Canada : Assurer l'avenir numérique du Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

4. The Register. Microsoft admet qu'il ne peut pas garantir la souveraineté des données de l'UE en vertu de la loi américaine, 2025. https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee

5. Heise Online. Not sovereign : Microsoft ne peut pas garantir que les données de l'UE restent en Europe, 2025. https://www.heise.de/en/news/Not-sovereign-Microsoft-cannot-guarantee-the-security-of-EU-data-10494789.html

6. Congrès des États-Unis. Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018. https://en.wikipedia.org/wiki/CLOUD_Act

7. Wikipédia. La loi de Moore. https://en.wikipedia.org/wiki/Moore%27s_law

8. Exploding Topics. Quantité de données créées par jour (2025). https://explodingtopics.com/blog/data-generated-per-day

9. Wevolver. The 2025 Edge AI technology report (rapport sur la technologie de l'IA de pointe en 2025) : L'avenir de l'Edge AI. https://www.wevolver.com/article/2025-edge-ai-technology-report/the-future-of-edge-ai