Le Cloud de l'État

Architecture d'une immunité numérique québécoise.

Le numérique québécois repose aujourd'hui sur une infrastructure qu'il ne contrôle pas. Les administrations publiques, les hôpitaux, les universités et une large part du secteur privé confient leurs données à trois entreprises américaines : Amazon Web Services, Microsoft Azure et Google Cloud. Ces trois acteurs, que l'industrie désigne sous le terme d'*hyperscalers*, concentrent environ 63% du marché mondial de l'infonuagique en 2025, selon les données de Synergy Research Group. Au Canada, les régions infonuagiques canadiennes d'AWS, d'Azure et de Google sont toutes des extensions directes de sociétés mères incorporées aux États-Unis, dans les États du Delaware et de Washington.

En 2018, le Congrès américain a adopté le *Clarifying Lawful Overseas Use of Data Act*, connu sous le nom de **CLOUD Act**. Cette loi contraint toute entreprise soumise à la juridiction américaine à **produire des données électroniques sur demande des autorités fédérales**, peu importe le pays où ces données sont physiquement stockées. Le mécanisme repose sur un principe appelé *jurisdiction by incorporation* : en droit américain, c'est le pays où une société est légalement enregistrée, et non l'adresse physique de ses serveurs, qui détermine quelle loi s'applique à elle. Un serveur situé à Brossard n'échappe pas à une injonction émise à Washington si l'entreprise qui l'opère est enregistrée au Delaware. Le CLOUD Act a été rédigé précisément pour que ce type de demande soit légalement irréfutable, quelle que soit la localisation physique des données, comme l'a confirmé la jurisprudence américaine dès 2018.

Le paradoxe québécois est donc le suivant : des données de santé, des dossiers fiscaux, des communications gouvernementales peuvent se trouver sur des serveurs physiquement localisés au Québec tout en demeurant accessibles aux autorités américaines sans qu'aucune procédure canadienne ne soit requise. Le mécanisme de notification prévu par le CLOUD Act est facultatif et ne constitue pas un droit de veto pour l'État concerné.

Ce constat mène à une distinction que la plupart des débats publics escamotent : la différence entre posséder un serveur et contrôler ce qui s'y exécute. Ce qui donne son utilité à un serveur, c'est le logiciel qui le fait fonctionner : d'abord l'hyperviseur (le programme qui permet à un seul serveur physique (ou une grappe) de faire tourner plusieurs machines virtuelles indépendantes, comme un immeuble divisé en appartements étanches), puis les couches logicielles supérieures. Si l'hyperviseur est un produit américain, l'opérateur québécois détient les clés du bâtiment physique mais loue le moteur à une entité juridiquement contraignable par Washington. Ce que les spécialistes désignent par l'expression de *backdoor légale* n'est pas une faille technique clandestine : c'est une obligation légale inscrite dans le cadre réglementaire auquel le fournisseur du logiciel est soumis. La souveraineté de la donnée exigerait que la chaîne logicielle complète repose sur des logiciels libres audités sans lien de dépendance envers une juridiction étrangère. Ce n'est pas réinventer la roue : des plateformes comme OpenStack pour la gestion infonuagique, ou KVM pour la virtualisation, sont des standards mondiaux maintenus par des milliers de contributeurs indépendants, utilisés par des dizaines de gouvernements. Comme le formule le juriste Bertrand Warusfel : *« La territorialité des données est une fiction juridique commode ; ce qui détermine réellement la souveraineté informationnelle, c'est la chaîne de contrôle des clés cryptographiques et l'identité juridique de celui qui les détient »* -- Bertrand Warusfel, *Droit et souveraineté numérique* (2021).

Le chiffrement souverain constitue la pièce centrale de cette architecture. Dans les infrastructures infonuagiques actuelles, les clés permettant de déchiffrer les données sont gérées par le fournisseur : AWS, Azure ou Google peuvent techniquement déchiffrer les données de leurs clients si une autorité compétente le leur ordonne. La solution s'appelle un HSM, ou *Hardware Security Module* : un composant matériel certifié qui génère et stocke des clés de chiffrement sans jamais les exposer à l'extérieur du dispositif, comme un coffre-fort dont la combinaison n'existe nulle part en dehors du coffre. Dans une architecture souveraine, les HSM seraient localisés sur le territoire québécois et opérés exclusivement par du personnel habilité. Même si un juge américain ordonnait la livraison de données hébergées au Québec, ces données seraient mathématiquement illisibles sans les clés, lesquelles ne relèveraient d'aucune juridiction américaine. C'est le modèle retenu par Thales dans son partenariat S3NS avec Google : les clés restent sous contrôle exclusif de Thales, société française non soumise au CLOUD Act. Cette protection ne tient cependant que si l'entité qui détient les HSM est elle-même hors d'atteinte du droit américain.

La seule réponse cohérente serait de rompre le lien de subordination juridique entre l'opérateur de l'infrastructure et toute entité soumise au droit américain, par la création d'une société d'État ou d'une coentreprise à majorité publique, incorporée exclusivement en vertu du droit québécois, sans actionnaire américain et sans contrat de licence créant un lien de dépendance envers une maison-mère étrangère. Les ingénieurs seraient des employés de droit québécois, les contrats de maintenance passeraient par des fournisseurs européens ou asiatiques, et l'infrastructure bâtie sur des standards ouverts resterait pleinement interopérable avec le reste du Web : l'étanchéité est juridique, non communicationnelle. Le modèle français Bleu, coentreprise entre Capgemini et Orange pour opérer Azure en France, bute précisément sur la limite inverse : la technologie sous-jacente reste américaine et soumise à licence. L'isolation juridique doit descendre jusqu'à la couche logicielle.

La question devient alors la suivante : comment convaincre des opérateurs dont la valeur repose sur des décennies d'intégration verticale d'accepter une telle rupture juridique ? La réponse se trouve dans ce que le Québec contrôle et qu'ils ne peuvent obtenir nulle part ailleurs. Le prix moyen du tarif industriel L d'Hydro-Québec s'établit à environ 5,8 cents CAD par kilowattheure en 2025, contre 7 à 12 cents dans la plupart des États américains et 15 à 20 cents en Europe occidentale, selon les données d'Hydro-Québec et de l'Agence internationale de l'énergie. L'énergie représentant entre 15% et 25% des coûts d'exploitation d'un grand centre de données, l'écart entre le Québec et la Virginie du Nord représente une économie annuelle de l'ordre de 15 à 25 millions de dollars américains pour un opérateur de 100 mégawatts.

Un gouvernement québécois souverain pourrait exercer ce rapport de force par un tarif souveraineté : un tarif préférentiel réservé aux opérateurs ayant accepté l'incorporation sous droit québécois sans actionnaire étranger, l'absence de tout contrat de licence créant une obligation de divulgation envers une maison-mère américaine, la gestion locale des clés cryptographiques, et la soumission exclusive aux tribunaux québécois. Ce mécanisme serait analogue à celui d'un port franc, et bénéficierait d'une assise juridique solide sous l'ACEUM, qui exclut explicitement les marchés publics de son chapitre sur le commerce numérique. Bernard Landry formulait ce principe dans sa généralité : *« La maîtrise de nos ressources naturelles n'est pas une question économique au sens étroit. C'est la condition matérielle de notre liberté politique. Un peuple qui ne contrôle pas ce que son sol produit ne contrôle pas non plus ce que ses institutions décident »* -- Bernard Landry, allocution devant le Conseil du patronat du Québec (2002). Microsoft ayant annoncé en 2023 un investissement de 3,2 milliards de dollars canadiens dans son infrastructure canadienne d'ici 2027, le marché québécois est un marché que ces entreprises ne pourraient pas abandonner pour une question de structure juridique locale.

L'absence d'un tel mécanisme a un coût que les budgets gouvernementaux enregistrent comme une dépense ordinaire, sans jamais la nommer : **une dîme**. Lorsque le gouvernement du Québec verse des centaines de millions annuellement à AWS ou à Microsoft, ces sommes financent indirectement le budget fédéral américain via l'impôt sur les sociétés, fixé à 21% depuis 2017. Une estimation construite à partir de données partielles de Statistique Canada situe le déficit annuel du Québec en services numériques à l'ordre de 4 milliards de dollars. Un CAPEX (dépense en capital) produit un actif durable inscrit au bilan de l'État ; un OPEX (dépense d'exploitation) disparaît sans laisser de trace patrimoniale. Construire un centre de données souverain de 10 à 20 mégawatts représenterait un investissement de 150 à 350 millions de dollars canadiens selon les données 2025 de Cushman & Wakefield, à mettre en regard d'un budget annuel du Centre de services partagés du Québec dépassant 800 millions, dont une part croissante part à l'étranger sans retour d'actif. En 2024, le coût moyen d'une violation de données au Canada s'établissait à 6,32 millions de dollars canadiens par incident selon IBM Security : une infrastructure souveraine, isolée des vulnérabilités communes aux installations des hyperscalers, réduit également cette exposition.

Ce raisonnement devrait orienter la séquence institutionnelle. La Loi 25, pleinement en vigueur depuis septembre 2023, régule les flux de données sans créer d'infrastructure souveraine. Les dossiers fiscaux, les dossiers de santé, les registres d'état civil et les communications des ministères régaliens constituent les quatre catégories à migrer en priorité : elles concentrent l'essentiel du risque stratégique. Un État qui ne peut garantir la confidentialité de ses propres fichiers fiscaux face à une puissance étrangère n'administre pas souverainement sa politique fiscale. Ce qui manquerait serait une loi-cadre définissant quelles données d'État ne pourraient être confiées qu'à des entités incorporées sous droit québécois exclusif, un mécanisme de certification des opérateurs, et une migration progressive par vagues. L'Estonie opère depuis 2007 une infrastructure d'État couvrant 99% de ses services publics. En 2017, elle a créé la **cyber-ambassade**, en hébergeant au Luxembourg des copies chiffrées de ses données d'État dans des serveurs bénéficiant d'une **immunité diplomatique complète** face à toute injonction étrangère.

Un Québec souverain disposant d'une telle infrastructure se trouverait dans une position que peu d'États peuvent offrir. Des dizaines de nations francophones et insulaires dont les données gouvernementales transitent par des infrastructures étrangères faute d'alternative représentent un marché diplomatique réel. Héberger leurs données dans une cyber-ambassade québécoise, sous un régime d'immunité diplomatique négocié bilatéralement, **générerait des revenus récurrents et ferait du Québec un fournisseur de souveraineté numérique**. Comme le formule l'économiste Diane Coyle : *« Les données sont la ressource naturelle du vingt-et-unième siècle, et comme toute ressource naturelle, la question centrale est de savoir qui en fixe les règles d'extraction »* -- Diane Coyle, *Markets, State and People* (2020).

Le CLOUD Act est un problème de droit, et les problèmes de droit se résolvent par du droit. La réponse complète combinerait une structure juridique étanche, une infrastructure physique souveraine bâtie sur des standards ouverts, un régime énergétique conditionnel, et une doctrine claire sur ce que l'État québécois accepte de confier à des tiers. L'Estonie, Singapour et la Suisse comptent parmi les États numériquement les plus souverains et les plus ouverts commercialement : l'ouverture viable repose sur le contrôle souverain, pas sur son absence.

Dans un monde où les données d'un hôpital, d'un fisc ou d'un état civil peuvent faire l'objet d'une injonction émise à des milliers de kilomètres, sans procédure contradictoire et sans droit de regard de l'État concerné, la question de l'hébergement physique et juridique des données cesse d'être une question informatique. Elle devient une question de sécurité collective, au même titre que le contrôle d'un réseau électrique ou d'une frontière. Ce qui reste à construire, c'est la décision politique de traiter la donnée publique comme ce qu'elle est : un bien collectif qui n'a pas à être administré sous la juridiction d'un autre État.

Louis-Martin Carrière