La souveraineté numérique, un concept à géométrie variable

Clément Gagnon
clement.gagnon@tactika.com
9 septembre 2025 / 2025-09-09T00:00:00Z

Le concept de souveraineté est ancien. La première mention connue est faite par Aristote dans l'ouvrage « Politique » (environ 300 ans av. J-C). Selon Wikipedia, la « souveraineté est un concept de philosophique politique désignant le concept d'autorité suprême, absolue et indépendante, exercée sur un territoire et/ou une communauté ».

Avant l'émergence des technologies modernes de communication, la souveraineté était associée à la notion de territoire. Il était aisé de délimiter l'application de la souveraineté d'un état dans un périmètre défini. Un état souverain édicte des lois qui sont en œuvre à l'intérieur de ses frontières. L'usage de la force « physique » (la guerre) étant le moyen ultime d'affirmer cette souveraineté.

Aujourd'hui, le concept de souveraineté s'applique dans trois grands domaines : Politique, Culturel(le) et Numérique.

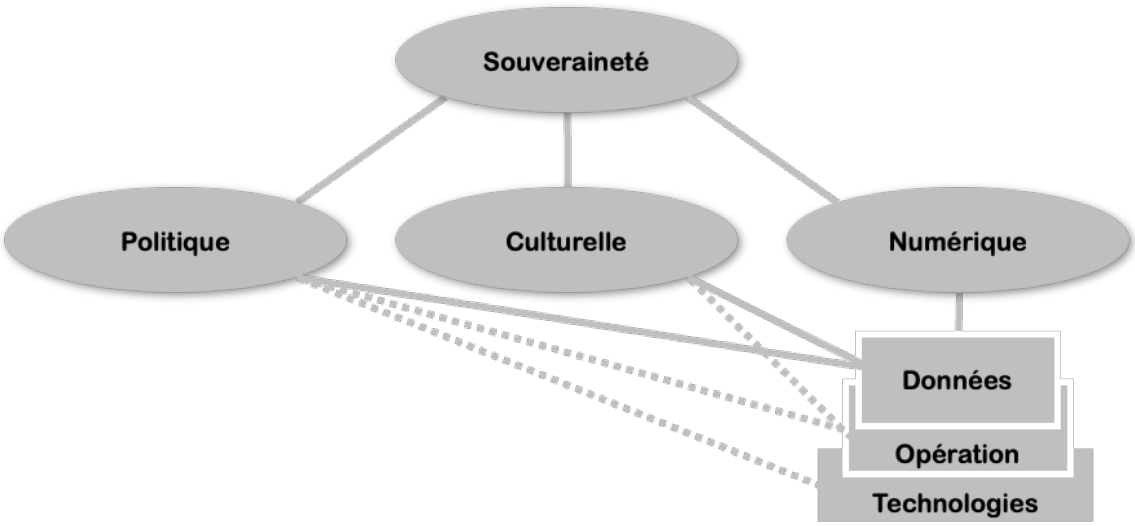

Figure 1. Cette figure illustre la relation entre les trois types de souveraineté.

La souveraineté politique se concrétise lorsqu'un état légifère afin de protéger et encadrer l'usage des données relatives à l'état et à sa population. Le système de justice est le moyen d'assurer cette souveraineté politique. Selon la situation, la souveraineté politique peut influencer les opérations et les choix technologiques en ce qui concerne la souveraineté numérique.

Le concept de la souveraineté culturelle est relativement récent. Il s'est défini après la Première Guerre mondiale grâce à une prise de conscience du pouvoir des médias et plus particulièrement de l'omnipotence de l'industrie audiovisuelle étasunienne. Cette forme de pouvoir est difficile à contrôler. L'émergence d'Internet au début des années 2000 a amplifié cette hégémonie à un niveau stratosphérique grâce aux réseaux sociaux.

La souveraineté numérique est plus complexe à définir. La consommation des médias d'information, d'art et de loisir s'appuie massivement sur le numérique. La souveraineté culturelle est liée à la souveraineté numérique sur plusieurs d'aspects et la souveraineté numérique est assujettie à la souveraineté politique.

Il faut mentionner que les États-Unis ne sont pas le seul acteur qui affecte la souveraineté numérique. La Chine est aussi un acteur actif avec ses réseaux sociaux (TikTok), ses plateformes de vente en ligne et autres moyens numériques (téléphone intelligent, IA, etc.).

Le domaine numérique peut être vu comme un modèle à trois couches ou niveaux : les Données, l'Opération et les Technologies.

Les Données (l'information) ne peuvent être utilisées qu'avec les Technologies et une gestion Opération/nelle des technologies et des données. Autrement dit, cela ne fonctionne pas tout seul !

La couche Opération est constituée de tous les moyens et processus nécessaires à gérer les Données et la couche Technologies.

La couche Technologies peut être simple ou très complexe selon le cas. Un cas simple est un fournisseur qui gère lui-même son infrastructure. Cette infrastructure contient du matériel (hardware) et du logiciel (software). Cependant dans les grandes organisations, la situation est plus complexe, nous y retrouvons souvent un mélange d'une infrastructure locale (qui est dans les murs de l'organisation) et des services infonuagiques provenant de gros fournisseurs (Microsoft, Amazon, Oracle ou des fournisseurs locaux, etc.). Pour compliquer

encore plus la situation, les logiciels (systèmes d'exploitation, hyperviseurs/virtualisation, base de données et etc.) peuvent provenir de fournisseurs étasuniens et être assujettis à leurs réglementations (Broadcom/Vmware).

La préoccupation envers la souveraineté numérique a pris de l'ampleur avec le constat du pouvoir des BAATMMAN (1) (les ex-GAFAM). Ces entreprises transnationales ont un énorme pouvoir qui s'exerce sur la planète entière. Certaines de ces entreprises font fi des lois des états souverains.

https://ici.radio-canada.ca/nouvelle/2157605/meta-elections-federales-desengagement-vote-information

Ces entreprises se permettent de faire des pressions politiques sur des états souverains. Certaines font un pillage des données personnelles afin de les exploiter sans aucune gêne.

https://www.ledevoir.com/monde/etats-unis/820195/etats-unis-accusent-geants-reseaux-sociaux-surveillance-masse

L'émergence de l'intelligence artificielle a ouvert un nouveau marché. Cette technologie a provoqué un pillage massif de la propriété intellectuelle pour entrainer les modèles de langage (LLM).

https://www.ledevoir.com/opinion/idees/869197/idees-impuissance-auteurs-face-intelligence-artificielle

Les actions récentes de l'administration trumpienne ont augmenté le niveau de stress envers la souveraineté numérique. Par un concours de circonstances de la politique américaine, ces entreprises se sont assujetties au pouvoir du président Trump.

Dans la majorité des scénarios, la souveraineté numérique est un enjeu lorsque des services infonuagiques sont impliqués. Les technologies et les opérations sont déléguées en tout en partie à des tiers ou des fournisseurs infonuagiques.

Souvent, il y a plusieurs tiers ou fournisseurs qui sont impliqués. En guise d'exemple, la figure suivante illustre un scénario répandu. Un utilisateur est un client d'un fournisseur canadien de services infonuagiques (en mode SaaS / Software-as-a-Service). Ce fournisseur canadien utilise des services infonuagiques de deux autres gros fournisseurs du GAFAM ou plutôt du BAATMMAN.

Dans ce scénario, bien que l'utilisateur utilise les services d'un fournisseur canadien, il peut être directement affecté par les décisions du gouvernement étasunien par l'intermédiaire des services consommés chez Microsoft et Amazon. Les données ainsi que les technologies peuvent en totalité ou en partie chez les fournisseurs étasuniens, mais les opérations sont canadiennes.

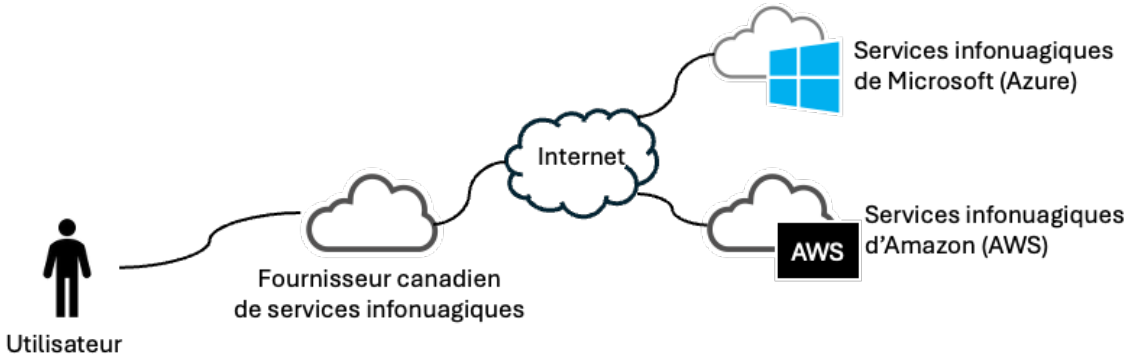

Figure 2. Cette figure présente un scénario d'un utilisateur canadien qui explite un service en mode Saas d'un fournisseur canadien mais en fait, il utilise (en totalité ou en partie) les services de fournisseurs étasuniens.

Une approche de la souveraineté numérique par les risques

Pourquoi se préoccuper de la souveraineté numérique ? La raison est qu'un état étranger (États-Unis) peut décider unilatéralement de l'usage et même de la pérennité de vos données.

Certes, il y a un cadre légal aux États-Unis (Cloud Act) pour l'accès aux données dans le cas d'enquêtes judiciaires chez les fournisseurs de service. Mais ne soyons pas dupe, il suffit d'invoquer la question de la sécurité nationale pour court-circuiter ce verrou légal.

Le discours du président Trump est de plus en plus agressif envers les nations qui légifèrent au sujet des services des géants étasuniens du numérique sur leur territoire.

Figure 3. Billet du président Trump qui menace directement de représailles les états qui veulent réguler les activités des GAFAM et autres fournisseurs de services Internet étasuniens.

Il y a un autre aspect dont on parle peu, la « disponibilité » des services des fournisseurs étasuniens. Ceux-ci peuvent être forcés de cesser de donner des services envers un individu, un groupe et éventuellement une nation.

Le schéma qui suit brosse un portrait des scénarios de risque où la souveraineté numérique est un enjeu.

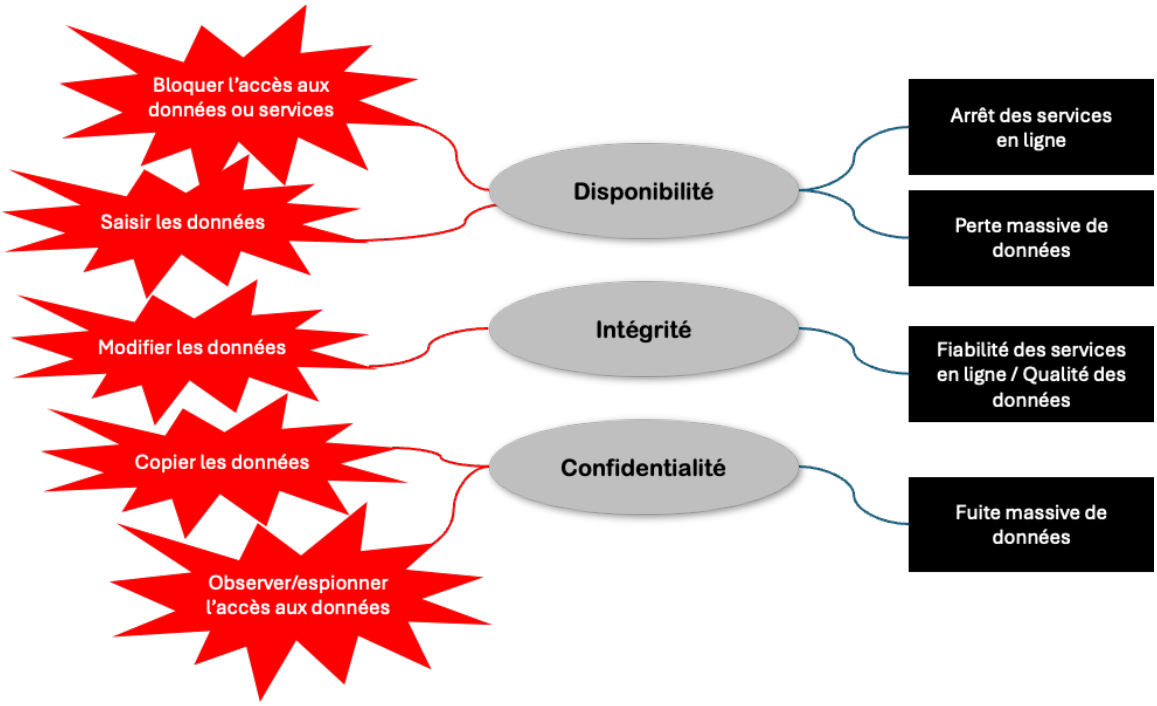

Figure 4. Illustration des scénarios de risque. Le lecteur doit noter que la probabilité n'est pas prise en compte dans cette illustration.

Dans le cadre de la souveraineté numérique, les scénarios de risque envers la disponibilité sont sous-estimés. La préoccupation de la plupart des acteurs est l'accès ou plutôt la copie des données.

Le blocage de l'accès aux services ou la saisie (destruction) des données sont possibles. Le résultat est tout simplement l'arrêt des services et éventuellement, une perte des données si un processus de copie locale de sécurité des données est absent.

Pour ceux qui croient que cette préoccupation est futile, il suffit de constater comment l'administration trumpienne fait pression sur un procureur de la Cour pénale internationale (blocage de l'accès à ses courriels et des comptes bancaires).

https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

Le scénario de risque qui concerne l'intégrité est sans doute celui qui a un degré de probabilité le plus faible (mais tout est possible à notre époque).

Imaginons ce scénario, notre gouvernement et notre industrie utilisent les données de géolocalisation par GPS dans plusieurs systèmes: l'industrie minière, les transports, l'aviation et etc.

Le système GPS est sous le contrôle total de l'armée des États-Unis. C'est un décret présidentiel qui rend le système GPS disponible à des fins civiles. Nous savons tous comment les décrets présidentiels sont à la mode à Washington. Il suffit d'imaginer le chaos si un changement de politique sur l'usage du système GPS traverse l'esprit du félon à la présidence.

https://www.gps.gov/policy/

La préoccupation en ce qui concerne la copie des données est une menace directe envers la protection de la vie privée et de l'usage à des fins mercantiles de ces données.

Le chiffrement est le moyen le plus efficient pour maitriser ce risque. Mais le chiffrement est un domaine complexe et compliqué. Il faut avoir de solides compétences en cryptographie. Une erreur dans ce domaine peut être fatale pour les données.

L'autre menace qui est malheureusement sous-estimée est la collecte d'information concernant l'accès aux données, les fameuses métadonnées. Dans certains cas, uniquement l'accès à ce type d'information peut constituer une fuite d'information.

Imaginons la collecte des accès à la boutique en ligne de la SQDC / Société québécoise du cannabis. Ces informations colligées avec celles des réseaux sociaux peuvent être colligées et être utilisées pour constituer une base de données afin de bloquer l'accès au territoire étasunien. Le Homeland Security a constitué une énorme base de données sur les individus, peu importe le pays d'origine.

https://www.dhs.gov/publication/dhstsapia-004-visitor-management-system
Il suffit de se remémorer de l'incident du site de la SQDC en 2018.

https://www.journaldemontreal.com/2018/10/29/lidentite-des-acheteurs-de-pot-a-risque

Que faut-il faire pour préserver et améliorer notre souveraineté numérique ?

La réponse à cette question est loin d'être facile. Tout dépend de la situation de l'utilisateur :

- Trouver des ressources compétentes;
- Lorsque la question du chiffrement est abordée, assurez-vous de comprendre les tenants et aboutissants, il ne faut pas croire aveuglément le discours des vendeurs de solutions;
- Comprendre les obligations légales;
- Favoriser des solutions technologiques de type logiciel libre;
- Challenger le fournisseur de service infonuagique sur l'enjeu de la souveraineté numérique;
- Imaginer le pire scénario (le pire va se concrétiser un jour ou l'autre);
- Toujours avoir des copies (récentes) de sécurité qui sont hors ligne.

Les fournisseurs de services infonuagiques (Microsoft, Amazon, Google, Oracle et autres) sont très conscients des enjeux et des contraintes associés à la souveraineté numérique. Chaque fournisseur propose des solutions qui faut évaluer soigneusement selon les risques.

Il ne faut pas oublier que dès qu'une entreprise étasunienne est impliquée dans la pile numérique (Données, Opération, Technologies), le risque envers de la souveraineté numérique existe.

---

(1) L'acronyme GAFAM (Google, Apple, Facebook, Amazon, Microsoft) est depuis longtemps employé mais l'acronyme BAATMMAN est le plus approprié ... pour le moment. L'IA est en train de bouleverser le marché.
BAATMMAN :

- B: Broadcom;
- A: Apple;
- A: Amazon;
- T: Tesla & X ;
- M: Microsoft;
- M: Meta (anciennement Facebook);
- A: Alphabet (maison mère de Google);
- N: NVIDIA.