La Souveraineté des Données et l’Espace Numérique

Le Cloud National et la souveraineté numérique.

La souveraineté numérique désigne la capacité réelle d'une collectivité politique à décider, appliquer et faire respecter ses règles dans l'espace numérique. Elle concerne des infrastructures concrètes, des choix technologiques précis et des rapports de pouvoir mesurables. Dans un monde où l'essentiel des activités économiques, administratives et militaires repose sur des systèmes informatisés, l'absence de souveraineté numérique équivaut à une dépendance structurelle aussi grave que la dépendance énergétique. Elle présente de surcroît une asymétrie que la dépendance pétrolière ne connaît pas : là où celle-ci se manifeste par des prix et des délais d'approvisionnement, la dépendance numérique peut se concrétiser instantanément, par une décision unilatérale prise à des milliers de kilomètres.

La souveraineté des données en est le socle. Elle signifie que les données produites par une société sont hébergées, traitées et protégées sous l'autorité exclusive de ses lois. Ce principe ne dépend pas du statut public ou privé de l'opérateur. Un cloud national peut être géré par un organisme gouvernemental, une société d'État ou une entreprise privée. Ce qui importe, ce sont trois critères vérifiables : l'infrastructure est située sur le territoire, elle est soumise au droit local, et aucun acteur étranger ne peut y accéder ou l'interrompre en vertu d'une loi externe.

Cette dernière condition est plus difficile à satisfaire qu'il n'y paraît. Deux types de dépendances entrent en jeu. La première est juridique. Le Cloud Act américain, adopté en 2018, oblige toute entreprise soumise à la juridiction des États-Unis à remettre des données à la demande des autorités fédérales, quel que soit le pays où ces données sont physiquement hébergées. Microsoft, Amazon et Google sont toutes concernées. Un ministère québécois qui confie ses dossiers à l'un de ces fournisseurs, même sur des serveurs situés à Montréal, reste potentiellement soumis à cette loi étrangère. La loi 25 du Québec, adoptée en 2021, impose des exigences strictes sur la protection des renseignements personnels, mais elle ne peut rien contre une injonction émise par un tribunal fédéral américain. La localisation physique des données ne garantit rien si l'opérateur est sous juridiction étrangère.

La seconde dépendance est technologique. L'analogie la plus directe est celle d'un réseau électrique : un État qui produit son électricité mais dépend d'un disjoncteur situé à l'étranger n'est pas souverain. En matière numérique, ce disjoncteur prend la forme de licences logicielles révocables, de mises à jour contrôlées à distance, ou de dispositifs matériels impossibles à auditer entièrement. En 2019, la décision du gouvernement américain de bloquer l'accès de Huawei à Android et aux puces TSMC a paralysé en quelques semaines le deuxième fabricant mondial de téléphones. Aucune clause contractuelle préexistante n'a pu l'empêcher. C'est la nature même de la dépendance technologique : une vulnérabilité que l'autre partie peut activer unilatéralement.

C'est là que les choix technologiques deviennent politiques. Les serveurs, routeurs, pare-feu, systèmes de sauvegarde et hyperviseurs utilisés aujourd'hui proviennent majoritairement d'entreprises américaines. Le Québec ne fabrique pas ces équipements. Même un cloud hébergé localement peut donc rester exposé à des décisions prises ailleurs. L'autarcie technologique complète n'est ni réaliste ni souhaitable, mais des orientations concrètes s'imposent : préférer les logiciels à code source ouvert dont le fonctionnement peut être vérifié et modifié indépendamment de l'éditeur, imposer que les données sensibles des administrations soient confiées à des opérateurs soumis exclusivement au droit local, et investir dans la formation d'ingénieurs capables de contrôler ces systèmes de l'intérieur plutôt que de les administrer depuis des interfaces fournies par des tiers. Ces orientations n'impliquent pas de rejeter les technologies étrangères en bloc, mais d'organiser leur usage de manière à conserver des points de contrôle effectifs.

Des tentatives en ce sens ont été menées avec des résultats contrastés. La France et l'Allemagne ont cherché à créer un écosystème cloud européen avec l'initiative Gaia-X. Le projet a rapidement révélé ses limites : Amazon et Microsoft en sont elles-mêmes devenues membres, diluant l'ambition de souveraineté en une certification d'interopérabilité. Cette dérive illustre la difficulté centrale : sans critères d'exclusion maintenus sous pression commerciale, les grandes plateformes absorbent les initiatives censées leur faire contrepoids. L'exemple, même dans sa forme négative, est instructif : la souveraineté numérique exige une définition précise de ce qu'on cherche à protéger et la capacité politique de tenir ces définitions dans la durée.

L'objection économique doit être prise au sérieux. Amazon Web Services, Microsoft Azure et Google Cloud proposent des services matures, fiables et souvent moins coûteux que leurs équivalents locaux. Mais les États ont régulièrement accepté des coûts supérieurs pour des secteurs jugés stratégiques. Airbus a absorbé des milliards de subventions publiques avant de devenir rentable. Hydro-Québec représente un actif dont la valeur stratégique pour l'autonomie économique du Québec dépasse largement sa rentabilité des premières décennies. La question n'est pas de savoir si un cloud souverain coûterait moins cher qu'AWS, mais si l'absence d'une telle infrastructure représente un risque acceptable. Confier les données fiscales, médicales et judiciaires des citoyens à des infrastructures soumises à un droit étranger revient à déléguer une partie du pouvoir régalien à des acteurs dont les obligations premières s'exercent envers leurs actionnaires et les lois de leur pays d'origine.

La souveraineté numérique n'est pas seulement défensive. Un État qui maîtrise ses infrastructures numériques est aussi en position de peser sur les normes techniques et juridiques qui structurent l'espace numérique mondial. Le règlement général sur la protection des données (RGPD) de l'Union européenne en est l'exemple le plus documenté : en établissant des exigences élevées, l'Europe a contraint des entreprises mondiales à adapter leurs pratiques à ses standards. C'est ce que la chercheuse Anu Bradford appelle l'effet Bruxelles dans The Brussels Effect (2020). On objectera que cet effet est contesté à mesure que d'autres grandes puissances développent leurs propres cadres : la Chine avec sa loi sur la protection des informations personnelles (PIPL), l'Inde avec son Digital Personal Data Protection Act. Cette objection renforce cependant le propos : ce sont précisément les États qui disposent d'infrastructures numériques souveraines et de marchés suffisamment importants qui participent à la formation de ces normes concurrentes. Les États sans ces capacités ne participent à aucun de ces débats ; ils subissent les règles des autres.

La capacité de peser sur des normes mondiales suppose qu'on contrôle ce qu'on met dans la balance. Dans le domaine militaire, cette réalité est encore plus brutale. Les systèmes militaires contemporains sont entièrement informatisés, et la dépendance technologique y prend une forme immédiatement stratégique. Le fonctionnement des avions de chasse F-35 dépend de logiciels propriétaires, de mises à jour centralisées et du système ALIS (désormais ODIN) contrôlé par Lockheed Martin. Des rapports du Government Accountability Office américain ont documenté à plusieurs reprises que les défaillances de ce système ont pesé sur le taux de disponibilité des appareils. Un État qui achète ces avions acquiert une capacité militaire assortie d'une contrainte permanente sur l'autonomie de son emploi. La dépendance technologique cesse d'être une vulnérabilité économique pour devenir une limite à l'autonomie de décision militaire, ce qui constitue une atteinte directe à la souveraineté dans son sens le plus classique.

Le politologue Bertrand Badie écrivait que « la puissance contemporaine ne repose plus seulement sur la force militaire ou économique, mais sur la maîtrise des dépendances » (L'impuissance de la puissance, 2004). Cette formule décrit exactement ce que l'Estonie a compris avant les autres. Elle avait déployé dès 2001 un système interopérable de services publics numériques (X-Road) et investi massivement dans sa résilience numérique. Quand elle a subi une cyberattaque nationale coordonnée en 2007, ces investissements ont prouvé leur valeur. Elle a depuis poussé la logique plus loin, en stockant des copies chiffrées de données d'État dans des ambassades de données à l'étranger pour préserver leur accessibilité en cas d'occupation physique du territoire. Cette approche, sans précédent dans le droit international au moment de son adoption en 2017, est aujourd'hui étudiée comme un modèle de résilience nationale.

Un projet d'État sérieux ne peut donc traiter le numérique comme un simple dossier technique à confier au fournisseur le plus compétitif du moment. Il s'agit d'un champ de souveraineté à part entière, au même titre que le territoire, la monnaie ou la défense. L'argument économique en faveur de la sous-traitance à des géants étrangers est réel mais incomplet : il mesure le coût de la souveraineté sans mesurer le coût de son absence, qui se paie en perte d'autonomie, en vulnérabilité exploitable et en incapacité à peser sur les normes qui régissent l'espace numérique. Sans maîtrise effective de cet espace, l'indépendance d'un État demeure partielle, conditionnelle, et réversible au gré des décisions prises dans des chancelleries étrangères ou des conseils d'administration dont les intérêts n'ont aucune raison de coïncider avec l'intérêt public.

Louis-Martin Carrière