# Une souveraineté numérique indispensable

Dans un contexte où le système d'information est vital et sensible au même titre que l'énergie et la santé, je vais dire quelques mots d'abord sur la souveraineté, et aussi sur l'autonomie stratégique. Je développerai ensuite quelques propositions et préconisations permettant de replacer la souveraineté sur l'aspect numérique, ses infrastructures et ses spécificités. Avec l'annonce de plusieurs axes à travers le Conseil National de la Refondation, ces préconisations permettront d'**aiguiller une politique volontariste pour aboutir à la souveraineté numérique, et une mise en œuvre au service du développement économique**.

## Souveraineté et espace stratégique numérique

Historiquement, la souveraineté est d'abord (16e siècle) assimilée au pouvoir absolu, illimité, qui établit la loi mais n'est pas contrôlé par la loi. Ce caractère absolu avec absence de contrôle évolue au siècle suivant avec les traités de Westphalie introduisant le concept d'État Nation, où la souveraineté est le moyen pour les princes et les États de revendiquer leur indépendance, qui devient un attribut de l'État souverain en droit international. La question a ensuite été de décider si les individus avaient certains droits naturels mais pouvaient en abandonner une partie au profit d'une autorité instituée par l'État, qui lui garantirait la protection et préservation de ses autres droits. Émerge un siècle plus tard la notion de contrat social, le dilemme étant de savoir s'il faut mettre une limitation morale, voire légale, à l'autorité instituée par l'État (c'est le débat quant à souveraineté nationale versus populaire).

Ces diverses acceptions étaient valables dans des environnements où les échanges entre environnements politico-économiques étaient maîtrisés en quantité et qualité. Ce n'est plus le cas aujourd'hui dans un monde ouvert, où l'incertain et le complexe règnent. Si du point de vue du droit international, tout État indépendant est souverain, la révolution numérique vient bouleverser les modalités de l'exercice de cette souveraineté du fait de ses activités transfrontalières, de l'interconnexion mondiale des réseaux, et des moyens d'action à distance.

Ce qui est dorénavant clé, est la **protection des intérêts de l'Etat**, et en particulier sa **continuité d'action en cas de crise**. Il faut donc identifier les événements potentiels susceptibles d'avoir un impact sur l'Etat, leur occurrence potentielle, et évaluer cet impact, c'est-à-dire évaluer son coût quant à la continuité d'action de l'Etat. Par exemple : quel est le coût de l'arrêt ou d'une malversation d'un service numérique clé s'il n'est plus disponible, tant individuellement (pour une industrie critique, un établissement public) que collectivement (au niveau de la société) ?

Notons que **la souveraineté numérique est évidemment un pan de la souveraineté économique et industrielle** : quels acteurs garder, préserver, coconner, développer, et à chaque fois pendant combien de temps ? Une question à se poser est aussi : quelle politique des brevets dans le domaine du numérique, pour garantir une protection des savoir-faire et des données, à des fins de production industrielle et d'exploitation commerciale ?

**Affirmer notre souveraineté numérique permet d'exercer notre autonomie stratégique**, c'est-à-dire le moyen pour un État d'exercer sa souveraineté, **afin de détenir la capacité autonome d'appréciation, de décision et d'action**. C'est le pouvoir du capitaine sur le bateau.

C'est dans le choix des **modalités d'indépendance et de dépendance, donc en fait d'interdépendance**, que réside l'autonomie de décision. Cela suppose d'avoir le choix entre différentes solutions technologiques viables industriellement et commercialement, au niveau national, pour pouvoir compter ensuite au niveau européen. Il paraît nécessaire de bâtir sur la complémentarité des stratégies nationales et européennes, la dimension européenne venant en complément et non en concurrence du niveau national. Encore faut-il avoir analysé et fait ses

propres choix capacitaires, s'approprier, pérenniser, renforcer certaines compétences de savoir et de savoir-faire.

Le constat est partagé par la grande majorité des acteurs : le numérique est devenu un instrument de puissance, et l'Europe a pris un retard du fait de son manque d'anticipation, d'où une dépendance à l'égard des puissances étrangères. Cette situation met potentiellement en péril la prospérité et la sécurité européennes. Par ailleurs il convient aussi de souligner une certaine indifférence citoyenne sur ces sujets : les matériels, les logiciels, les services numériques fonctionnent, pourquoi les changer, pourquoi changer nos habitudes ? Comme d'autres sujets, la question ne se posera au niveau du citoyen que le jour où il n'y aura plus accès…

Enjeu de souveraineté, enjeu de puissance, l'espace numérique est devenu progressivement décisif dans les rapports de force, tant pour les acteurs étatiques qu'industriels, et sa maîtrise est clé pour garder l'initiative, pour conserver l'autonomie de décision, pour réduire sa vulnérabilité. L'espace stratégique numérique peut être divisé macroscopiquement en trois domaines : les **données** qui sont le cœur de l'enjeu, les **applications** qui permettent leur traitement, les **réseaux** qui permettent les échanges et incarnent l'espace numérique.

**Chacun de ces trois domaines a ses propres enjeux de maîtrise**. Pour les données, il faut en maîtriser la quantité, la qualité, la propriété. Pour les applications, il faut également maîtriser les calculateurs et logiciels de nouvelle génération avec en particulier des capacités d'apprentissage, d'où des questions de maîtrise de la confiance. Enfin, pour les réseaux, c'est bien toute la dimension physique de bout en bout qu'il faut prendre en compte, à terre, en mer, dans l'air, dans l'espace, d'où une maîtrise de leur sécurisation, de leur intégrité, de leur approvisionnement énergétique le cas échéant.

Au-delà de ce triptyque simplificateur, il convient de noter que l'espace numérique est complexe, du fait de la diversité des technologies indispensables, de la dynamique d'évolution, et des interactions omniprésentes entre toutes les composantes. Les données sont contenues sur des supports physiques, traitées par des applications elles-mêmes constituées de données, les supports physiques et réseaux sont mis en œuvre par des applications elles-mêmes stockées sur des serveurs. Tout ceci exige donc une vision systémique de l'ensemble de l'espace numérique.

Une telle analyse doit de plus se faire sur toute la chaîne de valeur du numérique :

- **maîtrise des technologies**, au sens de la recherche et de la propriété intellectuelle ;
- **maîtrise de la production** de ces technologies, des produits et services associés ;
- **maîtrise de la vente et de la distribution** des produits et services.

Ces trois dimensions sont à considérer, de la même manière qu'une maison a des fondations, des murs, et un toit. En ce qui concerne la maîtrise des technologies numériques, elle doit s'analyser suivant différentes couches, un peu comme dans le modèle OSI :

- Électronique, matériels (disponibilité des matières premières, une filière de recyclage adaptée pouvant dégager des marges de manœuvre, conception et fabrication de composants clés) ;
- Infrastructures réseaux (intégrité des câbles sous-marins et terrestres, fibres, poteaux et antennes, 4G/5G/6G, satellites…) ;
- Logiciels de systèmes d'exploitation ;
- Environnements collaboratifs, Cloud ;
- Plates-formes d'accès (qu'elles soient publicitaires comme Google, nuagique comme Amazon, allégée comme Uber, industrielle ou de produits comme Mind-Sphere de Siemens : vous notez que c'est le seul domaine où j'ai trouvé un leader européen) ;
- Logiciels métier.

Mais si la maîtrise de certaines technologies est clé pour garantir la capacité à utiliser certains moyens d'action, encore faut-il savoir les produire, et ensuite les distribuer et en rendre possible l'accès. **La transformation numérique, c'est une recomposition des chaînes de valeur**, avec des consommateurs présents de plus en plus en amont, mais en fait aux différents maillons de cette chaîne : le BtoB devient du BtoC, du BtoBtoC, voire du BtoCtoB. Le client final prend une place centrale, c'est lui qui tire la valeur. Il ne faut plus penser produits, mais services et surtout usages.

Sous cet angle, qui n'est pas qu'une question technique, cela amène à regarder de près **les aspects de processus et de compétences**. La transformation numérique est trop souvent réduite à une révolution technologique : elle est avant tout humaine.

Le marché du numérique se compose d'une multitude d'acteurs de tailles très différentes ayant chacun un ensemble de compétences dans leurs spécialités respectives. Les domaines de la défense et de la sécurité ne font pas exception à cette règle. Comment donc former, attirer et conserver les compétences essentielles à notre souveraineté numérique ?

En effet, aujourd'hui, selon des rapports récents, près de trois quarts des entreprises ne trouvent pas, à l'heure actuelle, les professionnels dont elles ont besoin. La pénurie de ressources est aggravée par l'exigence, pour les acteurs du numérique œuvrant dans les domaines de la défense et de la sécurité, de pouvoir intervenir sur des sujets à forte sensibilité, avec des ressources humaines pouvant être habilitées, ce qui constitue une réelle contrainte.

Cette spécificité impacte le volume du vivier potentiel de compétences à toutes les étapes du parcours professionnel : formation initiale, recrutement des talents à leur sortie de formation, et rétention tout au long de leur carrière.

Pour faire face à cette demande et pour s'assurer que l'offre de formation soit adaptée aux besoins, il est indispensable de rapprocher les structures de formation initiale et les acteurs économiques (entreprises, organisations professionnelles, etc.). Des principes similaires peuvent et doivent être mis en œuvre pour la formation continue. Ainsi, les organismes de formation professionnelle pourraient également travailler en collaboration avec les fournisseurs de solutions souveraines dans une optique d'harmonisation entre l'enseignement initial et la formation continue.

Même s'il reste bien entendu des axes d'amélioration, la France dispose d'un vivier conséquent d'ingénieurs et de chercheurs, formés par les plus prestigieuses écoles scientifiques. Ce constat posé, l'enjeu est de retenir ces talents à leur sortie de formation en leur proposant des emplois et des parcours attractifs. Plusieurs critères apparaissent clé quant à la capacité à retenir les talents : le salaire ; les conditions de travail (matériel et humain) ; le sens et les perspectives de l'activité proposée ; la contribution au bien commun ; les engagements RSE.

Les domaines de la défense et de la sécurité rivalisent difficilement sur certains de ces critères : par exemple, sur les rémunérations « hors échelles » proposées par les géants Outre-Atlantique, ou sur certaines start-ups qui proposent des modèles de travail totalement disruptifs, même si ces deux dernières années ont entraîné des modifications importantes dans ce domaine, y compris au sein de l'administration. Il semble donc indispensable d'avoir une approche globale sur ces critères pour valoriser l'attractivité de ces domaines.

En termes de maintien des compétences numériques dans le temps (certains estiment que la durée moyenne de maintien de compétences numériques est aujourd'hui entre 2 et 3 ans !), il faut également faire évoluer les modes de management, et passer de la conduite à la culture du changement, avec l'objectif de former et faire évoluer les collaborateurs, quelle que soit leur position au sein de l'entreprise. Au sein du Ministère des Armées, est devenu à la mode le e-learning, et on va commencer le « reverse monitoring », c'est-à-dire que les « digital natives » vont apporter leurs connaissances aux cadres dirigeants, inversant dans le rapport mentor-mentoré la logique naturelle employeur-employé.

Je voudrais maintenant développer une stratégie de souveraineté numérique, en fait *un programme en 4 axes* pour construire, organiser, favoriser, la souveraineté numérique et sa mise en œuvre au service du développement économique de notre pays.

**<u>Une stratégie de souveraineté numérique en 4 axes</u>**

**Axe 1 :**

**Il faut définir les capacités clés à maîtriser au niveau national ; puis il faut les articuler selon des chaînes de valeur cohérentes**. Un tel exercice de définition capacitaire, accompagné d'une veille stratégique permanente, permet alors de choisir quoi préserver, quitte à renoncer à certains domaines accessoires ou inaccessibles.

En particulier, au niveau des infrastructures numériques, il est nécessaire de développer un réseau dédié, afin de protéger et sécuriser nos communications, nos données, nos informations, pour ne pas être exposé ou tenu par des conflits géopolitiques qui desserviraient l'intérêt de la nation. Cela renforcerait la maîtrise publique et la place de l'État, et permettrait de protéger son industrie et ses infrastructures dans les domaines de la santé, de l'énergie, de l'aéronautique et de la défense.

À l'instar de ce qui existe dans le domaine de l'énergie, où a été mise en place la Commission de la Régulation de l'Énergie qui a une mission de régulation des réseaux, concourt au bon fonctionnement des marchés et est au service de la transition énergétique, il serait nécessaire de créer un Secrétariat Général pour la Souveraineté Numérique et/ou une Commission de Régulation du Numérique.

En effet, la mise en œuvre efficace d'une politique de souveraineté numérique passe par une organisation alliant d'une part gouvernance et conduite, d'autre part centralisation des investissements et autonomie territoriale pour l'utilisation, afin d'éviter tant la dispersion initiale des efforts technologiques et industriels en conception et réalisation, que l'inertie ultérieure due à un dirigisme excessif ou une méconnaissance de spécificités territoriales en exploitation et utilisation. Créer un Secrétariat Général pour la Souveraineté Numérique permet cette coordination étroite des instances de gouvernance d'une part (pour les étapes de définition capacitaire et de construction budgétaire des axes de la politique de souveraineté numérique), et de conduite d'autre part (pour la mise en œuvre pratique d'une politique industrielle dans la définition et l'exécution des projets structurants via leur responsabilité contractuelle).

Par ailleurs, dans le cadre d'une mission de régulation du réseau numérique, la Commission de Régulation du Numérique élaborerait une tarification de l'utilisation des réseaux sécurisés et numériques qui prendrait en compte les évolutions des technologies, la sécurisation des réseaux, le stockage des données, les moyens humains pour la gestion et l'entretien des infrastructures autour des OIV (énergie, défense, santé, eau…).

**Axe 2 :**

**Suite à la réflexion capacitaire, une cartographie des acteurs industriels et étatiques est essentielle**, tant sur les technologies maîtrisées que sur les secteurs de vulnérabilité, sur les segments lacunaires mettant en danger certaines des chaînes de valeur, afin de **connaître les forces et faiblesses de l'empreinte française, voire européenne, dans l'espace numérique**.

Cette cartographie permettra de définir les urgences et les besoins pour créer le réseau des OIV de demain. Cela dessinera également les nœuds clés de ce réseau uniquement dédié aux services de l'État et aux secteurs définis comme OIV, avec un objectif de préservation des données et d'intégrité des infrastructures, pour éviter toute attaque cyber ou physique.

**Axe 3 :**

Ensuite, il faut d'une part être **prêt à certains efforts et certains sacrifices** ; d'autre part il faut **avoir les moyens de ses ambitions**, sur les différents plans intellectuel, technologique, financier, humain. Cela passe par :

- revoir les dispositifs visant à mettre en synergies les acteurs publics et privés,
- définir des modes de gouvernance appropriés,
- rechercher des proximités des acteurs, proximité se déclinant sur les axes de culture partagée, de valeurs partagées, de concentration géographique,
- mettre en place des structures coopératives dans la durée, sans tomber dans le piège des structures intégratives.

Pour avoir l'effet escompté, cette politique doit, sur le plan financier, **éviter tout saupoudrage et donc amener à des choix et des renoncements, assumés dans la durée**.

La dotation budgétaire pour les projets d'investissement numériques peut se faire par réorientation d'un pourcentage fixe à déterminer des budgets d'investissement des différents ministères, afin de s'assurer de la solidarité ministérielle et d'éviter des projets potentiellement concurrents favorisant la dispersion des efforts.

Puis, une fois les livrables des projets mis en production, le financement de leur utilisation serait à la charge de l'ensemble des acteurs publics (ministères, collectivités territoriales) et des opérateurs d'importance vitale, avec une double logique de forfait de base (proportionnel à la taille de l'acteur concerné) complété par un coût à l'usage. L'exploitation technique des livrables se ferait de surcroît dans un cadre de délégation de service public conforme à la politique industrielle numérique.

Évidemment, la viabilité de l'ensemble de ces mesures repose sur un cadre législatif astreignant les acteurs concernés à l'utilisation des ressources déployées.

Concernant la gestion, la modernisation, le déploiement de l'infrastructure de réseau numérique, c'est la Commission de Régulation du Numérique qui en assurerait la surveillance.

La gestion et l'exploitation de l'infrastructure seraient à la charge d'une entreprise dédiée (qui pourrait s'appeler RSF – réseaux sécurisés de France), où seraient présents l'État et la Caisse des Dépôts et Consignations. Cette entreprise aurait dans ses attributions le rôle d'entretenir, de moderniser et de faire le lien avec tous les utilisateurs afin de répondre à leur besoin. Elle devrait travailler avec l'ensemble des acteurs industriels français identifiés, et pourrait permettre de créer l'impulsion nécessaire pour faire travailler ensemble TPE, PME et groupes français afin de construire de véritables chaînes de valeur.

Il pourrait être envisageable de créer cette entreprise sur le site de Lannion, profitant d'une part de l'écosystème présent tant industriel (télécommunications, 5G, cyber) qu'universitaire, et permettant d'autre part de donner des perspectives dans l'intérêt du pays à des salariés locaux touchés récemment par plusieurs plans sociaux. Une telle densification autour des métiers et compétences permettrait aussi de renforcer une position où l'industrie est en faiblesse comme pour les semi-conducteurs, voire revenir à une position de leader sur l'innovation et la fabrication des matériaux pour le secteur du numérique.

**Axe 4 :**

Enfin, le dernier axe est **celui de la régulation et de son corollaire, la normalisation**. La souveraineté relève d'une capacité à réguler, et la régulation impacte la souveraineté quant à son influence sur la capacité à agir, c'est-à-dire sur l'autonomie stratégique. C'est alors une décision politique d'équilibrer le coût économique de la régulation par rapport aux bénéfices de la sécurité et la protection privée. Car réguler, c'est potentiellement se priver de certains bénéfices économiques de la connectivité, et poser une barrière à une expansion internationale.

La régulation peut venir tout autant par la normalisation que par l'outil juridique : une norme, c'est un condensé de l'état de l'art du moment, de recherche et développement, et de logique économique promue par un pouvoir public ou un privé ou les deux alliés, sur une fenêtre de temps ni trop courte ni trop longue. Arme économique pour celui qui la manie, c'est aussi un vecteur de fragilité pour celui qui la subit. En fait c'est un acte de confiance que de s'y plier, car on rentre de facto dans le jeu de celui qui a édicté, qui a concocté, ces normes ou ces lois. D'où l'impérieuse nécessité d'exercer cette volonté de normalisation et de régulation à une échelle suffisante, a priori européenne plutôt que nationale.

Il est intéressant de regarder rapidement cela à l'aune d'un exemple d'actualité. RGPD versus Cloud Act. Deux régulations relevant de deux philosophies politiques et économiques différentes. Le RGPD est un bouclier interdictif, limitant le champ d'action des acteurs étrangers à l'intérieur de sa zone géographique d'origine, bref il relève de la défense. Le Cloud Act est une arme intrusive, renforçant le champ d'action des acteurs étrangers à l'extérieur de sa zone géographique d'origine, bref il relève de l'attaque.

Naturellement, ce rôle de régulation relèverait du Secrétariat Général pour la Souveraineté Numérique, ou de la Commission de Régulation du Numérique qui aurait en son sein des personnels avec une expertise pouvant analyser les actions au service de la gestion, du déploiement et de l'exploitation de l'infrastructure des réseaux sécurisés de France.

Voilà, en quelques mots, ma vision de la souveraineté numérique et de sa mise en œuvre possible à court et moyen termes.

Comme mot de fin, je rappellerai deux citations que l'on attribue à Einstein :
*« Rien ne se passe jusqu'à ce que quelque chose bouge. »*
*« La folie, c'est de faire toujours la même chose et de s'attendre à un résultat différent. »*