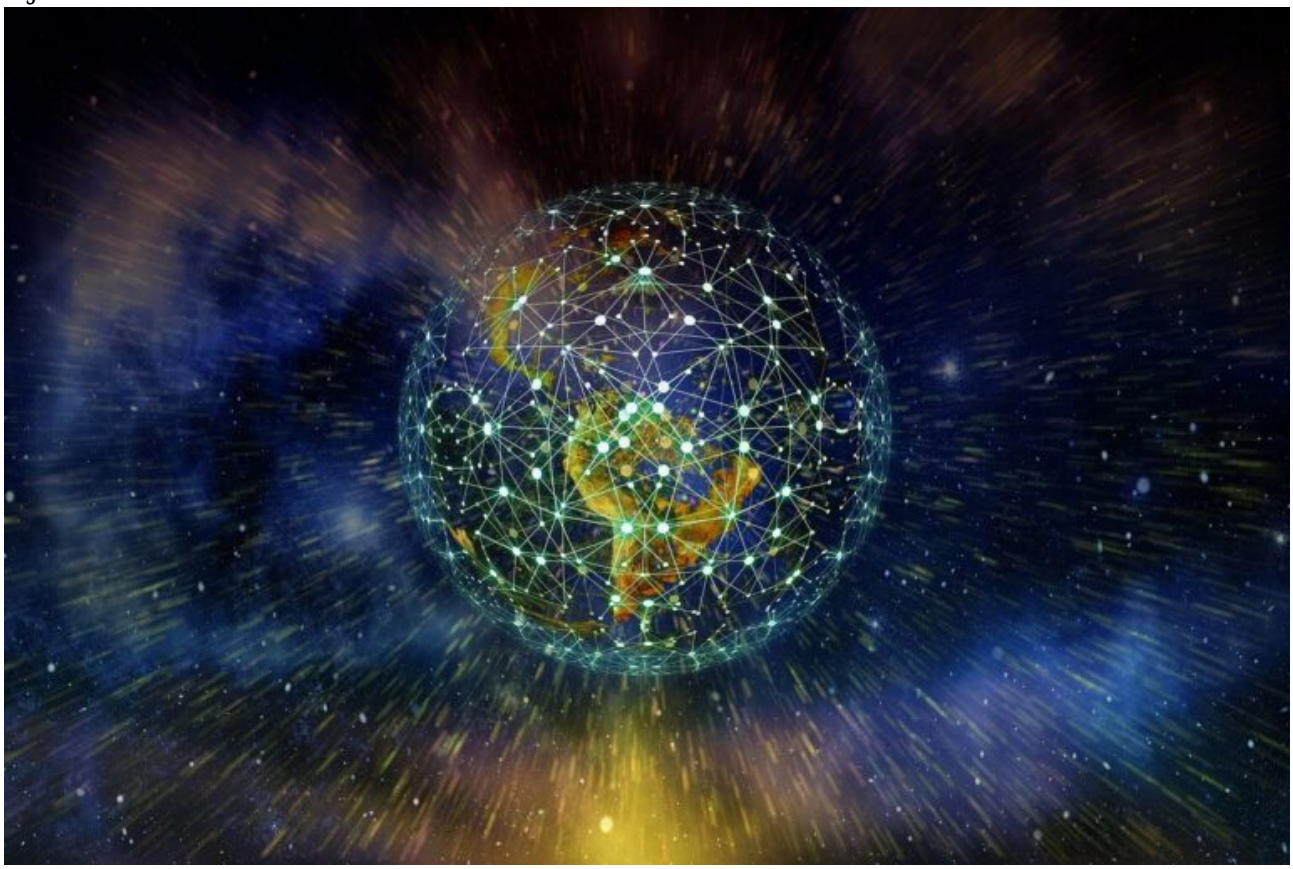
Conférence d'Alain Juillet : "Fondements et frontières de la souveraineté numérique"

Category: 2020-2030,Actualités,Alain Juillet,Souveraineté
1 janvier 2025



Le monde est en train de changer en passant de la domination des occidentaux à celle des BRICS. Parallèlement après avoir cru à la mondialisation depuis 1990 nous rentrons dans la multipolarité dans laquelle chaque groupe de pays veut affirmer sa spécificité et recouvrer une souveraineté mise à mal par le système occidental.

La souveraineté c'est le droit absolu d'exercer une autorité législative, judiciaire ou exécutive sur une région, un pays ou un peuple. Comme l'a défini le général De Gaulle : Tout système qui consisterait à transmettre notre souveraineté à des aéropages internationaux serait incompatible avec les droits et devoirs de la république française.

Au niveau d'un pays elle peut être politique, territoriale, économique, militaire et, pour ce qui nous intéresse, numérique.

A ce stade il faut rappeler la définition du numérique : c'est une information qui se présente sous forme de nombres, associés à une indication de la grandeur physique à laquelle ils s'appliquent, permettant les calculs, les statistiques, et la vérification des modèles.

La souveraineté numérique c'est donc tout ce qui permet à un état ou une organisation d'établir son autorité, pour exercer ses pouvoirs dans le cyberespace, en couvrant des domaines comme le contrôle des données personnelles ou la dépendance technologique.

Pour aller plus loin il faut se souvenir qu'elle est de deux ordres :

- La souveraineté numérique proprement dite concerne la propriété et fait référence à la capacité de gouverner l'infrastructure numérique. Elle permet de donner confiance aux citoyens, aux entreprises et aux administrations en contribuant à la protection de leurs données personnelles, professionnelles ou étatiques. On la mesure en identifiant au niveau des fournisseurs, des technologies, et des personnes, les endroits où un effet de verrouillage ou d'autres problèmes affectent ou peuvent affecter la souveraineté numérique

- La souveraineté des données concerne le contrôle. Elle fait référence aux lois et à la gouvernance entourant la collecte et le stockage des données. Elle repose sur l'autorité permettant de détenir des données et sert en droit générique au service des nombreux aspects liés au traitement des données numériques entre protection chiffrement transmission et stockage.

En France la RGPD établit ce qui est acceptableen matière de collecte de traitement et de stockage des données personnelles. On attend des entreprises qu'elles respectent la vie privée, qu'elles soient transparentes sur la manière de collecter et d'utiliser les données, et qu'elles leurs fournissent les outils dont elles ont besoin pour gérer leurs données.

Au niveau de l'UE dans le cadre du *Digital Cyber Act* mis en marche le 6 mars 2024, le commissaire européen Thierry Breton a fait adopter 3 textes : le *Digital Operational Resilience Act* (DORA) pour les financiers, le *Digital Service Act* (DSA) pour les contenus illégaux , et le *Digital Market Act* (DMA) pour protéger les utilisateurs européens et leurs données.

Cette souveraineté des données de l'UE est garantie par l'application de ces réglementations assurant leur protection quel que soit leur lieu de traitement ou de stockage.

Elle développe la concurrence sur les marchés numériques avec les géants du secteur. Sa mise en œuvre au niveau des enquêtes qui démarrent va permettre des sanctions réelles : ainsi Apple risque 6% d'amendes sur son CA mondial pour abus de monopole. Mais les capacités de remplacement des GAFAM par des acteurs européens est loin d'être évidente d'autant que la commission se mobilise peu pour y contribuer comme on l'a vu par exemple pour Nokia.

En complément de la souveraineté numérique et des données, il faut évoquer l'IA souveraine qui est la capacité d'une nation à développer l'IA avec des talents locaux à différents niveaux, en fonction de sa stratégie nationale en matière d'IA. Elle fait référence au contrôle exercé par un gouvernement ou une organisation sur les technologies d'IA et les données pour l'adapter à ses besoins locaux en vue de préserver ses valeurs et sa surveillance réglementaire.

Comme l'a dit Joseph Wehbe au *World Economic Forum* de Davos : Tous les gouvernements devraient travailler à lancer et développer des ecosystèmes d'IA locaux pour piloter la compétitivité économique et préserver leurs propres valeurs.

Selon la définition de Francois Jolain, la souveraineté numérique repose sur 3 piliers :

– l'électronique que l'on fabrique (hardware)
– les logiciels qui tournent (software),
– les logiciels qui offrent un service en ligne sur internet (cloud)

Le Hardware :

C'est la filière des infrastructures commençant par les serveurs dans les datacenters reliés par des câbles de fibres optiques à travers le monde et se terminant en périphérie par tous les appareils connectés.

Les GAFAM et les BATX investissent dans les infrastructures. Les câbles sont surveillés et interceptés non seulement par les pays traversés mais aussi sur leur parcours sous-marins.

L'ensemble repose sur l'utilisation massive de semi-conducteurs. Il y a quelques années Intel contrôlait la chaine avec un quasi-monopole. Aujourd'hui c'est très fragmenté mais la majeure partie de la fabrication se concentre sur l'Asie, principalement à Taiwan avec TSMC, Foxcom, et Mediatel mais il y en a aussi en Corée, au Japon, et en Chine avec Huawei.

La clé du process est dans la réalisation des puces. Les schémas de base sont vendus par ARM ou RISC-V en open source. La fabrication passe par un producteur sélectionné pour sa capacité selon l'épaisseur en nanomètre sachant que plus les transistors du circuit électronique sont fins plus on peut densifier le circuit et dissiper la chaleur. La plupart des producteurs font des puces de 7nm, soit environ 10.000 fois moins que l'épaisseur d'un cheveu, qui répondent à des besoins courants.

Les Hollandais d'ASML sont les seuls à faire des machines de gravure de 5nm. En position quasi monopolistique puisqu'elle est la seule capable de fabriquer des puces de 5nm, TSMC est localisée dans la zone conflictuelle de Taiwan. Pour préserver la souveraineté numérique des occidentaux, les Américains ont obtenu la création de deux usines dans l'Arizona qui seront opérationnelles fin 2026. l'UE a également obtenu qu'une usine soit construite en Allemagne. Parallèlement on est obligé de constater que, depuis l'interdiction d'achat de puces taiwanaises et de machines ASML imposée par les Américains, la Chine rattrape son retard plus vite que prévu grâce à de très gros investissement dans la recherche avec l'aide de l'espionnage technologique.

Dépendre de puissances étrangères pour le *hardware* ouvre la porte à la surveillance et aux interceptions. On l'a vu avec Cisco pour la 4G et Huawei pour la 5G. Pour limiter le risque il faut avoir des entreprises capables de concevoir et de produire en France, comme ST Micro appuyé par des labos de recherche comme le CEA Tech à Grenoble qui intéresse nos concurrents.

Le Software :

Il existe autant de logiciels tournant sur le *hardware* que d'usage, les plus critiques étant les systèmes d'exploitation (OS). Chacun crée une sorte de monopole car leurs applications sont conçues pour cet OS. De surcroit, plus il y a d'utilisateurs plus il y a d'applications ce qui attire plus d'utilisateurs. Le meilleur exemple est Microsoft qui propose un OS avec son ensemble d'applications permettant de répondre à tous les besoins.

Tout OS permet d'espionner son utilisateur directement ou par des *back doors*. C'est dans le *software* qu'apparaissent chaque semaine 5 000 virus nouveaux qui peuvent piller, détourner, copier ou détruire les données, ou encore organiser des demandes de rançons. Leur capacité peut aller jusqu'aux destructions massives avec des virus type *Scada* comme *Stuxnet* et *Olympic Games* qui peuvent détruire des usines iraniennes ou couper des sources d'énergies comme la lumière de villes ukrainiennes.

D'un autre côté l'exploitation des failles des OS et des applications ouvre des possibilités qui justifient les travaux de recherche pour les détecter et les éliminer. L'open source qui réduit une partie du danger et de la dépendance est devenue la norme la plus utilisée. La Gendarmerie française qui utilise un OS, basé en open source, sur Linux en est un bon exemple.

Le Cloud

Les Américains ont été les premiers à créer des *clouds* pour stocker des datas et créer nombre de services et logiciels en ligne. Le problème est venu des lois extraterritoriales des Etats-Unis qui permettent aux Services et administrations de pouvoir consulter et copier tout ce qui passe à travers ou utilise un élément américain.

De surcroit les différences de conception de la donnée, protégée en Europe mais commercialisée aux USA fait que des opérateurs comme, par exemple, Facebook, Tik tok ou Waze aspirent les données quand on les utilise.

Au-delà de son utilité indiscutable, le *cloud* est donc un endroit dangereux pour la sécurité des données si l'on n'y prend pas garde. Il faut toujours vérifier où sont localisés les *datacenters* et connaitre l'origine et les fonds du propriétaire du *cloud*. Ce risque réel a provoqué la création de *clouds* souverains européens et nationaux aux résultats variables car la concurrence est rude avec ceux d'outre atlantique qui sont en général moins coûteux et plus performants.

En réalité, si l'on veut vraiment sécuriser ses données, la solution passe par une évaluation hiérarchisée des données mises dans le *cloud*. On peut confier à un *cloud* américain ou international celles dont la diffusion ne représente aucun risque, à un *cloud* national celles qui sont très importantes ou essentielles, et à un *cloud* européen celles qui sont entre les deux.

La pratique montre que nous en sommes loin pour deux raisons ;

- Après l'échec du projet *Andromède,* la France ne dispose que d'un nombre très restreint de *clouds* souverains performants. De plus on est obligé de constater que les tentatives d'entrées en bourse d'OVH pour se renforcer ont été perturbées selon un processus que l'on a déjà connu chaque fois que cela pouvait pénaliser des entreprises américaines.
- En dépit des alertes et sensibilisations l'Etat et de nombreuses grandes entreprises

continuent à traiter avec des *clouds* et des sociétés américaines dans des domaines variés comme la santé les impôts ou les énergies.

Au-delà du législatif, incluant la certification et les réglementations en vigueur, de l'optimisation de la chaine opérationnelle, et de la protection des données, le maintien de la souveraineté numérique implique l'utilisation de la cyberdéfense défensive et offensive face aux prédateurs de toute sortes et de toutes origines. Face à une évolution continue des technologies et des modes d'actions utilisés par les Etats, certaines entreprises et les groupes criminels, c'est un complément indispensable pour sécuriser sa position, qui utilise des outils conçus pour cette mission.

L'efficacité de la cybersécurité suppose une définition des objectifs à atteindre, un cadrage du périmètre et une identification préalable des vulnérabilités de l'entreprise. A ce stade il faut viser large en commençant par les modes de travail, les outils et leur utilisation, les bonnes pratiques, sans oublier les actions de prévention. Il ne faut jamais oublier que sans une politique de prévention on subit. Ajoutons que le développement de la mobilité et des outils nomades renforce l'importance des communications sécurisées et les risques d'interceptions.

Vouloir une souveraineté numérique demande non seulement d'anticiper mais aussi de répondre aux attaques qui se multiplient. Ainsi en 2023 :

- 69% des attaques ciblaient des entreprises
- 20% des collectivités territoriales
- 11% des établissements de santé

Sommes-nous numériquement souverains quand :

– en janvier 2024 l'hôpital Simone Veil de Cannes est attaqué par un ransomware et le groupe Ramsay santé subit une attaque conjointe dans deux établissements

– en février France Travail subit un malware infiltré ses systèmes informatiques

– en avril Saint-Nazaire subit une attaque qui paralyse les systèmes d'information et les services municipaux tandis qu'à Pont-à-Mousson la communauté de communes doit faire face à un cryptovirus

– en mai Engie subit une cyberattaque du groupe Lapsus tandis qu'Intersport se fait voler 52 Go de données sensibles.

– et pendant tout ce temps la SNCF et la Société générale affrontent des actions de pishing sur les clients qui continuent encore aujourd'hui

Les fondements et les frontières de la souveraineté numérique concernent aussi bien la data que la régulation, l'innovation que la cyberdéfense, sans oublier la puissance numérique dans tous les domaines que nous venons d'évoquer. Leur énumération et les problèmes rencontrés

démontre qu'il est impossible pour un pays comme la France mais également pour l'Europe de contrôler toute la chaine. Notre souveraineté ne peut donc être totale. Elle ne peut être que partielle et sélective car certaines composantes doivent être partagées ou transférées. C'est à travers la liberté de choisir ce qui est transférable que s'exerce la véritable souveraineté. Le but ultime étant la protection du pays et la capacité d'assurer les fonctions essentielles à son bon fonctionnement. Cette option est donc réalisable en se focalisant sur certains niveaux et certains domaines comme les logiciels dans le *software* et dans le *cloud* ou sur des secteurs stratégiques.

Mais n'oublions pas l'évolution permanente des techniques et outils. L'arrivée du quantique risque de remettre en cause toute une partie de notre analyse et des éléments potentiels de souveraineté. Pouvant gérer d'énormes ensembles de données beaucoup plus efficacement, il va changer notre futur technologique dans de nombreux secteurs. De surcroit, il faut être conscient que ces innovations et leurs applications variées vont être amplifiée par l'intelligence artificielle.

Alain JUILLET
Conférence prononcée par le président de l'AASSDN
Producteur de la chaine Open Box TV
http://openboxtv.fr/emissions/