La souveraineté numérique: enjeux et défis

Professeur Yacine Challal
Ecole nationale Supérieure d'Informatique, (ESI-Alger)
Laboratoire de Méthodes de Conception de Systèmes (LMCS)

Résumé

Dans cet article, nous allons présenter les enjeux et défis de la souveraineté numérique. Pour cela, nous présenterons la genèse du cyberespace pour mieux appréhender les enjeux politiques et économiques derrière l'expansion hégémonique de cet espace. Puis nous présenterons les enjeux et défis de la souveraineté numérique illustrée par certaines expériences de construction de cette souveraineté. Nous terminons cet article par une analyse PESTEL (Politique, Economique, Sociale, Technologique, Environnementale et Légale) de la souveraineté numérique pour saisir les défis de ce concept à différentes échelles et l'importance d'élaborer une stratégie globale pour acquérir cette souveraineté.

Mots clés : Cyberespace, Souveraineté numérique, Protection de données personnelles, Auto-détermination informationnelle.

ملخص

في هذا المقال، سنعرض رهانات وتحديات السيادة الرقمية. لهذا الغرض سنتطرق إلى نشأة الفضاء السيبراني من أجل فهم أفضل للرهانات السياسية والإقتصادية الكامنة وراء اتساع نطاق هيمنة هذا الفضاء. ثم سنتحدث عن رهانات وتحديات السيادة الرقمية التي تجسدها بعض التجارب في بناء هذه السيادة وفي الأخير سنقوم بتحليل سياسي، إقتصادي، إجتماعي، تيكنولوجي، بيئي وقانوني للسيادة الرقمية من أجل إستيعاب تحديات هذا المفهوم على مستويات مختلفة وأهمية وضع إستراتيجية شاملة لإكتساب هذه السيادة.

الكلمات المفتاحية: الفضاء السيبراني، السيادة الرقمية، حماية البيانات الشخصية، تقرير المصير المعلوماتي.

Introduction

Le cyberespace est devenu aujourd'hui un espace de prédilection, d'influence politique, économique et socioculturelle. En vingt ans de développement d'Internet, nous avons assisté, parfois impuissants, à une métamorphose spectaculaire d'un réseau de transmission de données entre des ordinateurs, vers un espace, sans frontières, de confrontation géopolitique capable de détruire des pays, de changer des régimes, d'influencer des élections d'Etats souverains et basculer des sociétés dans le chaos.

Devant l'emprise de sociétés, principalement américaines, sur cet espace devenu stratégique, et leur pouvoir grandissant avec des visées hégémoniques, plusieurs nations et organisations transnationales (Russie, UE, Chine, Association des Nations de l'Asie du Sud-Est, Inde, …) militent depuis le début des années 1990 pour une gouvernance transparente et multilatérale d'Internet et du cyberespace. Ceci a fait émergé le concept de souveraineté numérique selon des dimensions diverses (juridique, politique, économique, culturelle, …) et une finalité unique qui est de permettre l'auto-détermination informationnelle à différentes échelles : individuelle (protection des données personnelles), nationale (souveraineté des Etats dans le cyberespace), et transnationale (défense des intérêts économiques et politiques d'organisations transnationales).

1. Souveraineté nationale vs. pouvoir hégémonique des GAFAM

La souveraineté est traditionnellement définie par « l'autorité suprême dans un territoire. L'Etat est l'institution politique dans laquelle la souveraineté est matérialisée »[1]. Cette notion classique de souveraineté est aujourd'hui disputée aux Etats par des entreprises multinationales avec des visées hégémoniques offrant à leurs adeptes, clients et victimes des services de substitution aux Etats comme des identités numériques, des monnaies électroniques, des ressources financières en contreparties d'activités virtuelles, et une aura dans une société virtuelle transnationale. « La souveraineté traditionnelle est remise en cause, dans une société dite post-westphalienne caractérisée par l'interdépendance des Etats, la montée en puissance des organisations internationales, la mondialisation économique, le développement des échanges transnationaux, et désormais la globalisation engendrée par des technologies qui échappent largement aux Etats, et se jouent des frontières physiques »[2].

En effet, depuis les années 2000, des sociétés multinationales, principalement américaines comme les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), NATU (Netflix, Airbnb, Tesla, Uber) et un peu plus tard leurs équivalents chinois BATX (Baidu, Alibaba, Tencent, Xiaomi), forment une oligarchie du cyberespace. Leur puissance économique rivalise avec les puissances économiques mondiales comme les Etats-Unis d'Amérique, la Chine ou le Japon comme on peut le constater sur la comparaison de la valorisation boursière des GAFAM et le PIB de certaines puissances économiques sur la Figure 1. Nous constatons par exemple que la valorisation des GAFAM en bourse est supérieure au PIB du Japon ! et celle de Google supérieure au PIB d'un pays comme le Pays bas !

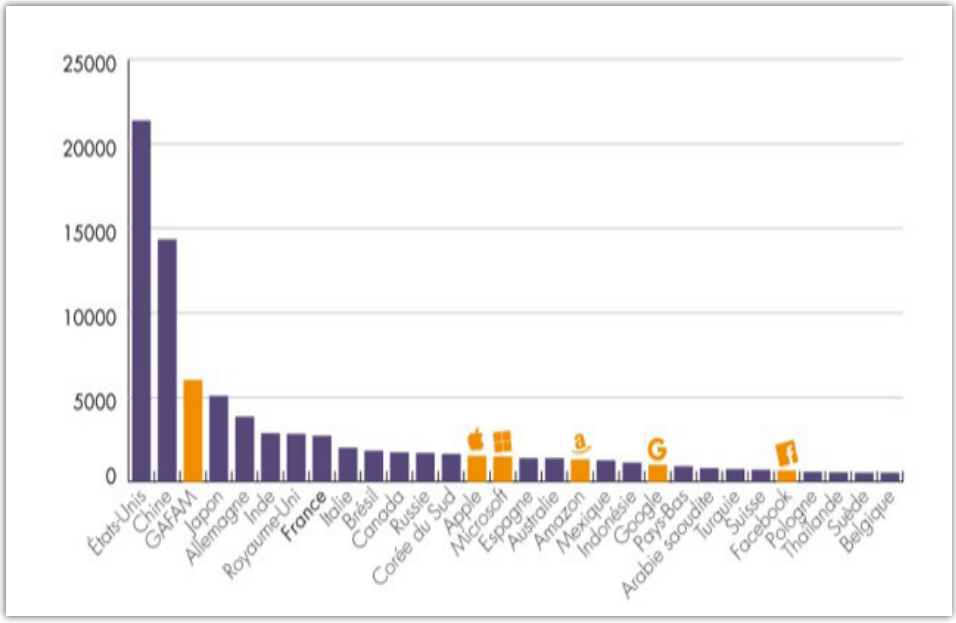

Figure 1: Comparaison PIB 2019 et valorisation boursière des GAFAM en milliards de dollars au 10 juin 2020 (source la financepourtous.com d'après la banque mondiale et bloomberg)

La puissance économique de ces entreprises hégémoniques leur confère aussi une puissance politique les hissant au pouvoir d'organisations souveraines transnationales disputant même la souveraineté des Etats nations.

Ces entreprises règnent sur le cyberespace et décident du sort des données personnelles avec des visées économiques et politiques allant

jusqu'à la déconstruction des Etats et la fabrication de régimes dans le sillage d'une stratégie géopolitique dont les ficelles sont tirées par les pays hôtes de ces entreprises ou des entités malveillantes non-identifiées.

2. Le cyberespace : enjeux des frontières

2.1. Genèse du cyberespace et sa nature transfrontalière

Internet est né de l'interconnexion de réseaux distants. Il avait pour objectif le partage des capacités de calcul offertes par des ordinateurs puissants à une communauté d'utilisateurs en vue d'y effectuer des calculs intensifs et traitements de données nécessitant des capacités d'exécution et de stockage élevées.

Le développement de l'infrastructure d'Internet et son interconnexion aux réseaux de télécommunication, le développement de la filière des smartphones (des ordinateurs miniaturisés) et des objets connectés, ont donné une nature ubiquitaire à Internet.

Cette omniprésence d'Internet dans les sphères économiques, sociales et privées a encouragé le développement de services indénombrables et a constitué un levier important pour le développement économique et social des sociétés contemporaines.

Avec ces services de toutes natures (économiques, sociaux, médiatiques, culturels, etc.), Internet s'est métamorphosé vers un cyberespace à part entière, dont l'existence et viabilité, la rentabilité, et la puissance sont dues essentiellement à sa nature transfrontalière qui lui procure sa matière première d'une façon abondante: les données de ses utilisateurs. Ces données constituent l'essentiel des actifs immatériels de cette entreprise hégémonique qu'est le cyberespace. La loi qui règne dans cet espace échappe au contrôle des peuples et aux Etats et se matérialise sous forme d'algorithmes et de codes informatiques[3]. La nature globale du cyberespace se manifeste selon plusieurs aspects :

2.1.1. Aspects techniques

Internet est une technologie globale par essence. C'est une des manifestations de la globalisation et un espace où la mondialisation prend tout

son sens. En effet, les fournisseurs de services requièrent des emplacements physiques pour accueillir leurs serveurs pour stocker et traiter les données. Les centres qui abritent ces serveurs sont communément appelés « data centers ». Ces « data centers » sont distribués à travers le monde et se voient déployés là où se trouve une infrastructure adéquate, une énergie peu coûteuse et des compétences locales pour les administrer et les maintenir en marche. Selon ces critères, ce ne sont pas toutes les localités du monde qui sont en mesure d'accueillir des « data centers »[4].

Ainsi, tout pays ou organisation connecté à Internet et consommant des services du cyberespace, concède implicitement une partie de sa souveraineté sur les données qu'il met à disposition des fournisseurs de services dont les data centers sont localisés hors de ses frontières. Cet état de fait a poussé certains pays ou organisations transnationales (comme l'Union européenne) à défendre le principe d'extra-territorialité de leurs lois et règlements régissant la protection des données personnelles de leurs citoyens.

Par ailleurs, la nature distribuée d'Internet est un facteur essentiel pour la robustesse des transmissions et la continuité de services. Grâce à cette nature distribuée, même si un composant d'Internet se verrait défectueux, les paquets de données pourront emprunter d'autres routes redondantes et arriver à destination malgré la panne de certains composants d'Internet.

Les flux de données sont davantage complexes et distribués quand on considère le commerce électronique : l'acheteur et le vendeur peuvent être dans des pays différents, et verront les données issues de leur transaction traverser plusieurs autres pays pour accomplir la transaction. L'entreprise qui héberge la plate-forme e-commerce, les institutions financières, « data centers » et l'hébergeur web, peuvent être tous dans des pays différents comme illustré sur la Figure 2 [4].

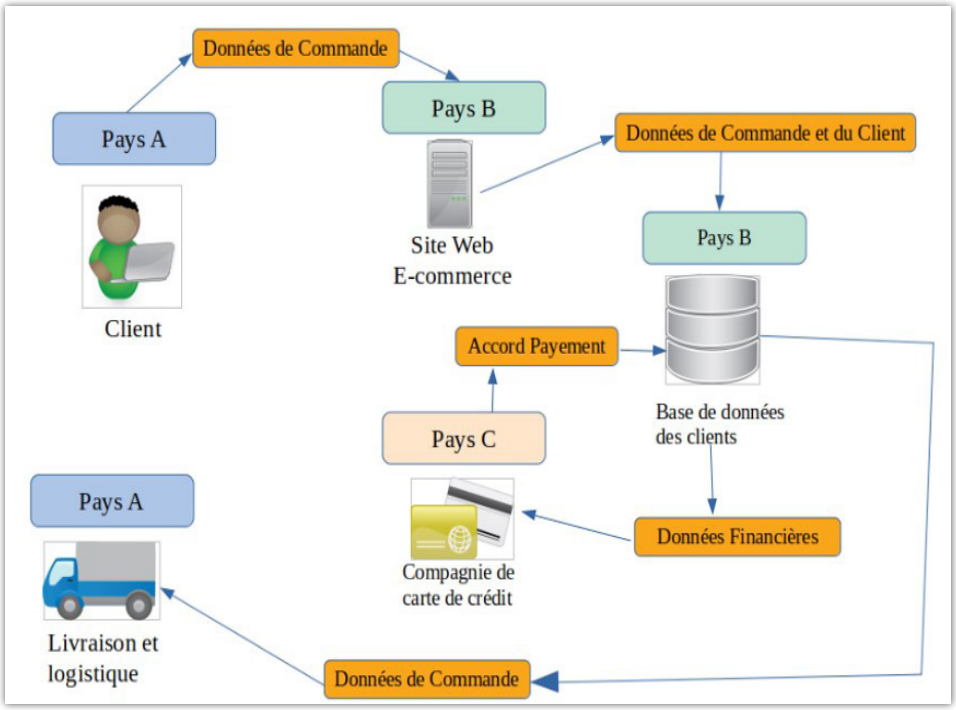

Figure 2: Nature distribuée d'Internet, du cyberespace et de ses services[4]

2.1.2. Aspects socio-économiques

Le cyberespace est aujourd'hui indéniablement un espace mondial de création de richesse, d'emploi et d'échange. Il s'agit d'un levier important pour le développement économique, l'efficacité des services publics et de prospérité socio-économique en général. Il est important de considérer cette réalité, malgré l'exploitation de cet espace à des fins hégémoniques et de déstabilisation par certaines entreprises et entités, pour élaborer une stratégie de construction d'une souveraineté numérique efficace avec lucidité.

En effet, ces dernières années Internet a évolué vers un Internet des objets/Internet of Things (IoT), aspect essentiel du cyberespace, intégrant tout objet communicant et couvre ainsi un large éventail d'applications (comme illustré par la Figure 3) et touche quasiment à tous les domaines que nous affrontons au quotidien. Cet IoT augmenté d'algorithmes de l'intelligence artificielle et d'analyse de données, permet l'émergence

d'espaces intelligents autour d'une informatique omniprésente. Parmi ces espaces intelligents, on peut citer :

- Les villes : l'IoT permettra une meilleure gestion des réseaux divers qui alimentent nos villes (eaux, électricité, gaz, etc.) en permettant un contrôle continu en temps réel et précis. Des capteurs et algorithme d'optimisation permettent d'améliorer la gestion des parkings et du trafic urbain et diminuer les embouteillages et les émissions en CO_2;
- L'énergie : la gestion des réseaux de distribution de l'énergie se verra améliorée grâce à la télémétrie (smart grid), permettant une gestion en temps réel de l'infrastructure de distribution de l'énergie et permet l'intégration des énergies renouvelables malgré leur instabilité dans le temps. Cette interconnexion à large échelle facilitera la maintenance et le contrôle de la consommation et la détection des fraudes;
- Le transport : dans ce domaine l'IoT constituera un prolongement naturel des « systèmes de transport intelligents » et leurs apports en termes de sécurité routière, confort, efficacité de la gestion du trafic et économie du temps et de l'énergie;
- La santé : dans le domaine de la santé, l'IoT permettra le déploiement de réseaux personnels pour le contrôle et le suivi des signes cliniques, notamment pour des personnes âgées. Ceci permettra ainsi de faciliter la télésurveillance des patients à domiciles, et apporter des solutions pour l'autonomie des personnes à mobilité réduite. Dans le sillage du développement de la 5G, des applications de télémédecine (diagnostic et intervention) sont envisageables grâce à la réduction des délais de transmission et l'augmentation des débits. Des algorithmes issus de l'intelligence artificielle ont été conçus pour le dépistage précoce de plusieurs types de cancers ou le diagnostic de pathologies à partir de l'imagerie médicale;
- L'industrie : dans l'industrie l'IoT permettra un suivi total des produits, de la chaîne de production, jusqu'à la chaîne logistique et de distribution en supervisant les conditions d'approvisionnement. Cette traçabilité de bout en bout facilitera la lutte contre la contrefaçon, la fraude et les crimes économiques transfrontaliers;
- L'agriculture : dans ce domaine, des réseaux de capteurs interconnectés à Internet peuvent être utilisés pour la supervision de l'environnement des cultures. Ceci permettra une meilleure aide à la décision en agriculture, notamment pour optimiser l'eau d'irrigation, l'usage des

intrants, et la planification de travaux agricoles. Ces réseaux peuvent être aussi utilisés pour lutter contre la pollution de l'air, du sol et des eaux et améliorer la qualité de l'environnement en général.

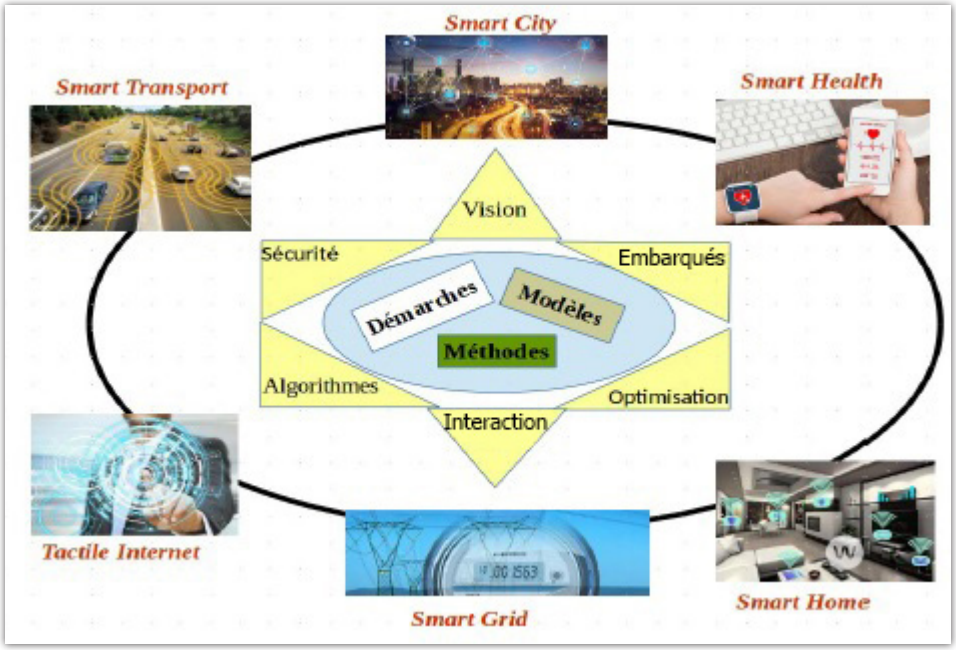

Figure 3: L'Internet des objets, l'Intelligence artificielle et la création d'espaces intelligents

Ces exemples d'applications montrent que le cyberespace peut contribuer à améliorer la qualité de vie des personnes, en créant de nouveaux marchés, de nouveaux emplois, des débouchés et de la croissance pour les entreprises, et un élan pour la compétitivité.

Internet, et ses applications citées ci-dessus, reposent essentiellement sur la circulation des flux de données, le plus souvent d'une façon transfrontalière, pour les raisons techniques citées dans la section précédente et pour des raisons économiques en lien avec la taille des marchés et la rentabilité des investissements consentis.

2.1.3. Aspect juridique

Un vide juridique a encouragé les dépassements que nous connaissons aujourd'hui dans le cyberespace en lien avec la cybercriminalité ou l'expansion hégémonique de certaines entreprises pour des fins géopoli-

tiques. « En l'absence de régulations nationales, les compagnies interagissant avec les utilisateurs dans le cyberespace n'étaient guidées que par certains principes internationaux de protection des données personnelles comme ceux élaborés par Asia Pacific Economic Cooperation (APEC), Organization for Economic Cooperation and Development (OECD) ou le Conseil de l'Europe. Les gouvernements et les citoyens ont réalisé récemment que la régulation n'a pas suivi l'évolution des technologies dont le modèle économique repose sur l'analyse de données et l'extraction de connaissances de celles-ci ; des données récoltées essentiellement de l'interaction des utilisateurs avec ces compagnies en ligne. Ainsi, les gouvernements réalisent l'importance de la régulation de la collecte et traitement des données »[4].

2.1.4. Aspects politiques et culturels

La collecte, l'analyse et le traitement des données générées par les activités de prêt de 5 milliards d'internautes constituent le processus de forage et de raffinement du 21ème siècle. Dans ce marché, une situation de quasi-monopole d'entreprises (essentiellement américaines), leur confère un pouvoir d'influence politique et culturel sur nos sociétés. Elles décident selon des algorithmes mis en œuvre par ses ingénieurs des règles de censures de contenus, de distillation d'idées et idéologies via les millions de pages consultées au quotidien, et de suggestions de contenus et de produits via les réseaux sociaux et moteurs de recherches. Elles conservent et analysent les données personnelles de milliards d'internautes souvent à leur insu.

Par ailleurs, plusieurs études ont démontré l'influence des réseaux sociaux sur les communautés et individus[5]. Ceci a été exploité à maintes reprises pour déstabiliser des gouvernements, influencer le cours d'élections et créer des atmosphères de méfiance et de chaos dans les sociétés. Ce mode opératoire de conflits, dis de cinquième génération, exploite pleinement le cyberespace et les réseaux sociaux en particulier pour vaincre des territoires ennemis sans recourir aux armes. Il s'agit de guerre d' « information et de perception »[6] .

2.2. Enjeux d'extension de la souveraineté des Etats au cyberespace

La liberté de développement qu'a eu Internet durant les années 1990 a permis de bâtir un nouvel espace économiquement prospère. Une lourde régulation au début de développement d'Internet aurait freiné son développement[7]. Cependant, Internet est aujourd'hui un des secteurs économiques qui génèrent le plus de profits, et au vu de l'exploitation de cet espace par des acteurs ambigus ou non identifiés ou malveillants pour mener des actions de déstabilisation à grande échelle pour des fins qui ne servent pas l'intérêt général, sa régulation devient un impératif sociétal et une responsabilité des Etats pour protéger leurs citoyens.

Cette volonté d'étendre la souveraineté des Etats au cyberespace s'est matérialisée sous le concept de souveraineté numérique.

2.2.1. Définition de la souveraineté numérique

James Andrew Lewis définit la souveraineté numérique par « le droit d'un Etat à gouverner ses réseaux pour servir ses intérêts nationaux, notamment la sécurité, la protection des données personnelles et son économie »[7].

Bernard Benhamou la définit par la capacité à «maîtriser l'ensemble des technologies, tant d'un point de vue économique que social et politique», et de «se déterminer pour avoir sa propre trajectoire technologique» [8].

Il s'agit de deux définitions complémentaires, car l'affirmation de l'autorité de l'Etat sur le cyberespace ne peut être réelle et efficace qu'à l'issue d'une maîtrise de ses technologies et infrastructures informationnelles.

L'expression de «souveraineté numérique» est utilisée dès 2012 lors de la Conférence mondiale des télécommunications internationales, notamment par la Russie et la Chine qui revendiquent la restauration de leurs «droits souverains» sur la gestion du réseau et l'élaboration d'un traité international permettant de mieux partager les responsabilités[2].

Dans ce qui suit, nous illustrons les efforts réalisés par certains Etats, organisations internationales et transnationales en matière de souveraineté numérique :

2.2.2. Expérience de l'Union européenne

Constatant la dominance des Etats-Unis et de la Chine sur l'économie numérique en général et des données en particulier, l'Union européenne a mis en place un règlement régissant la protection des données personnelles : General Data Protection Regulation (GDPR)[11]. Cette loi effective depuis 2018, exige aux entreprises interagissant avec des citoyens européens via le cyberespace, quelle que soit leur localisation physique, à leur délivrer un contrôle total sur leurs données personnelles en les informant des traitements prévus sur leurs données et en leur offrant la possibilité de refuser ces traitements et de supprimer leurs données collectées. Il s'agit du principe de consentement éclairé de l'utilisateur quant au traitement et stockage réservés à ses données collectées lors de son interaction avec ces services dans le cyberespace. La GDPR stipule aussi l'extra-territorialité du règlement qui exige les mêmes droits aux citoyens européens vis-à-vis de fournisseurs de services localisés en dehors de l'UE quand ils interagissent avec des citoyens européens et des résidents de l'UE.

Sur un autre volet, consciente de la domination des compagnies non-européennes sur les technologies de stockage et les services cloud, l'UE a lancé l'initiative de création d'une infrastructure fédérées de data-centers conformes à la GDPR : GAIA-X[4].

Ces deux volets législatif et technique affirment la volonté de l'UE à recouvrer sa souveraineté numérique d'une manière assez subtile et sans affront avec la globalisation. Il s'agit d'un choix stratégique conforme à l'esprit de l'alliance transatlantique.

2.2.3. Expérience de la Chine

La Chine a opté pour un modèle de souveraineté plus affirmée sur le réseau au sein de ses frontières. Au centre de la stratégie numérique de la Chine, on retrouve un contrôle de l'espace numérique, en termes de contenu, par le gouvernement, la protection des données et le traitement préférentiel des entreprises locales. Trois lois concrétisent cette stratégie : Cyber Security Law (CSL-2016), Personal Information Protection Law (PIPL 2020) et Data Security Law (DSL-2021)[4].

Par ailleurs, la Chine a encouragé le développement de ses propres entreprises pour faire face à l'hégémonie américaine et fournir un substitut de services conformes à la réglementation chinoise et affirmant la souveraineté numérique chinoise.

Ainsi, BATX (Baidu : moteur de recherche, Alibaba : e-commerce, Tencent : réseaux sociaux, Xiaomi : smartphones), l'équivalent chinois des GAFA n'est pas moins puissant en capitalisation boursière comme on peut le voir sur la Figure 4.

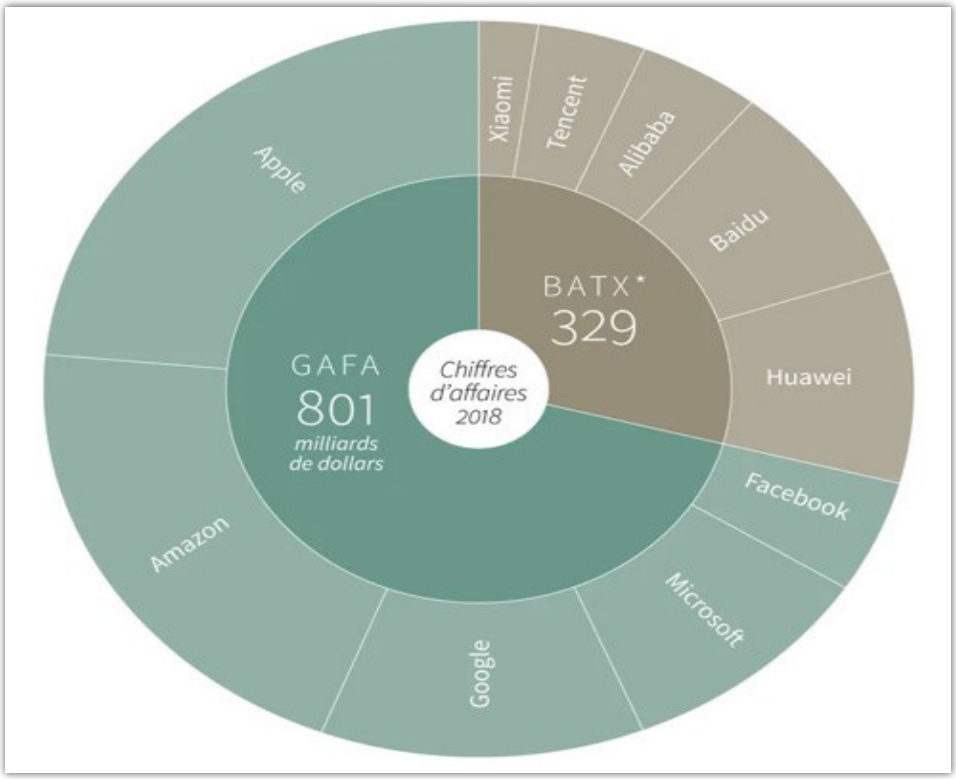

Figure 4: Les revenus des GAFAM et des BATX (Crédits : Sabrina BLANCHARD, Thomas PERROTEAU / AFP)

2.2.4. Avancées à l'ONU

Lors de la 68ème session de l'Assemblé générale des Nations unies (2013), le groupe d'experts gouvernementaux sur les développements dans le domaine de l'information et télécommunications dans le contexte de la sécurité internationale, recommande la reconnaissance du principe de souveraineté numérique. En effet, la 20ème recommandation stipule que la souveraineté de l'Etat et les normes et principes internationaux qui découlent de la souveraineté, s'appliquent à l'action de l'Etat dans les activités en lien avec les technologies de l'information et de la communication, et à leur juridiction sur les infrastructures TIC au sein de leur territoire[9].

L'inscription du concept de souveraineté numérique dans l'agenda de l'ONU est un pas important vers l'instauration d'une régulation globale du cyberespace dans le respect de la souveraineté des Etats.

3. La souveraineté numérique: se construit et se fait respecter

Dans cette section, nous allons synthétiser les enjeux et défis de la souveraineté numérique sous forme d'une analyse PESTEL (Politique, Economique, Sociale, Technologique, Environnementale et Légale). Cette synthèse, illustrée à la Figure 5, permettra d'appréhender la souveraineté numérique avec lucidité en considérant une approche globale prenant en compte les différentes dimensions de cette analyse.

3.1. Dimension politique

L'enjeu de la souveraineté numérique du point de vue politique est la restauration du contrôle de l'Etat sur ses infrastructures TIC au sein de son territoire et l'usage qui est fait des données personnelles de ses citoyens. Un autre enjeu est de faire face aux guerres de 5ème génération, aux « fake news », aux discours de la haine et aux opérations de déstabilisation orchestrées à partir du cyberespace. Le défi majeur est que le rapport des forces est nettement défavorable aux Etats (écart important dans la maîtrise des technologies, situations de monopole, lieu de stockage des données, tribunaux compétents, extra-territorialité, etc.)[2].

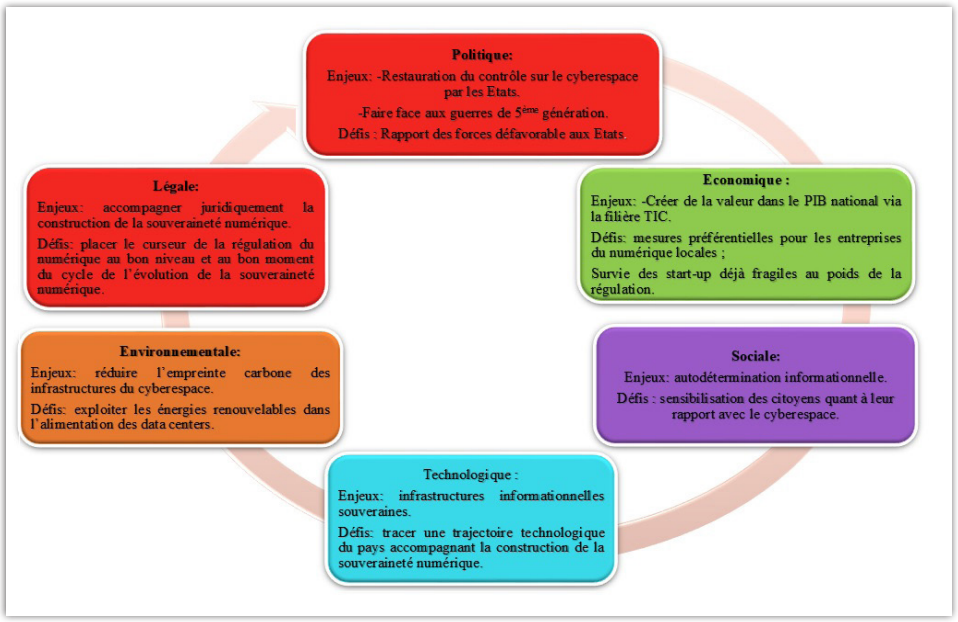

Figure 5: Synthèse d'une analyse PESTEL sur la souveraineté numérique.

Afin de renverser ce rapport de force, il serait nécessaire d'élaborer une stratégie à long terme permettant de surmonter les défis sus-mentionnés: maîtrise des technologies, localisation du stockage des données aux frontières nationales, mesures préférentielles pour les entreprises nationales du numérique, création de services de substitution aux produits des multinationales hégémoniques. A court terme, les Etats n'ont le choix que d'occuper le cyberespace avec une communication proactive, efficace et crédible. Un alignement sur des règlements ou « frameworks » internationaux en lien avec les principes de protection des données personnelles et l'affirmation de la souveraineté individuelle sur les données personnelles aiderait à faire face au pouvoir des multinationales hégémoniques.

3.2. Dimension économique

L'enjeu du point de vue économique est de créer de la valeur dans le PIB national à travers les activités économiques dans le cyberespace. Les multinationales qui détiennent actuellement le monopole, échappent aux différentes taxes en profitant de domiciliation de leurs entreprises dans des paradis fiscaux. Le défi est donc de réussir à mettre en place des mesures préférentielles pour les entreprises du numérique localisées dans les frontières nationales. Mais un autre défi surgit alors qui consiste à déployer l'infrastructure TIC requise pour localiser ces activités dans les frontières nationales. Le risque d'affirmer les souverainetés nationales dans le cyberespace est de créer des frictions dans la connectivité globale, ce qui impacte négativement la circulation des flux de données nécessaires à l'industrie du numérique.

Environ 80 pays ont fait passer des lois qui restreignent les flux de données transnationaux. Parmi ces restrictions, on retrouve le contrôle des données personnelles, des données comptables et financières, des données gouvernementales et des données des impôts. La localisation des données ne va pas découper Internet ou la « balkaniser », ça va compliquer le modèle économique des multinationales hégémoniques. A long terme, ces frictions vont faire perdre des opportunités de marchés à de nouvelles et/ou petites entreprises[7] [4] .

3.3. Dimension Sociale

L'enjeu vis-à-vis de la dimension sociale est de préserver le droit des personnes à l'autodétermination informationnelle. Ceci appuie le droit des personnes à contrôler l'usage réservé à leurs données personnelles qu'elles génèrent dans le cyberespace. Ceci se traduit par des lois sur la protection des données personnelles comme la loi algérienne n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel[10], ou la GDPR (UE)[11]. Le défi serait de sensibiliser les citoyens à mesurer l'importance de l'identité numérique qu'ils construisent dans le cyberespace. «Si elles ne veulent pas subir l'évolution technologique, les jeunes générations doivent apprendre à maîtriser les outils numériques, à connaître et faire valoir leurs droits et libertés, et à se préoccuper de la construction et de la protection de leur "identité numérique", générée par l'ensemble des traces laissées volontairement ou non sur les réseaux »[2].

3.4. Dimension Technologique

L'enjeu de la souveraineté numérique du point de vue technologique est de disposer d'infrastructures informationnelles souveraines dans les frontières nationales pour accompagner la souveraineté numérique dans ses dimensions légales, politiques, sociales et économiques. En effet, tous les Etats et organisations transnationales qui défendent le concept de souveraineté numérique ont élaboré des stratégies pour leur indépendance technologique sur tous les plans: « data centers » souverains (comme l'infrastructure GAIA-X de l'Union européenne), systèmes d'exploitation qui équipent les dizaines de millions des ordinateurs personnels et gouvernementaux (comme Astra Linux en Russie, ou Kylin en Chine), moteurs de recherche souverains pour stocker les traces des citoyens dans les frontières nationales et préserver leurs autodétermination informationnelle (comme Yandex Russe, ou Baidu Chinois), réseaux sociaux souverains (comme vKontakte Russe ou WeChat et Weibo Chinois). Le tableau à la Figure 6 synthétise certaines initiatives de développement de logiciels souverains.

Type	Chine	Russie	France
Système d'exploitation	Kylin (basé sur FreeBSD) puis Ubuntu Kylin (basé sur Linux Ubuntu) : https://www.ubuntukylin.com	Astra Linux : http://www.astra-linux.ru	CLIP OS (Noyau Linux) https://www.ssi.gouv.fr/administration/services-securises/clip
Moteur de recherche	Baidu : https://www.baidu.com	Yandex : https://yandex.com	Qwant : https://www.qwant.com
Réseaux sociaux	**WeChat : www.wechat.com** **Weibo : www.weibo.com**	**Vkontakte : https://vk.com/**	/

Figure 6: Logiciels souverains par pays

Le défi est de réussir à tracer la trajectoire technologique d'un Etat pour bâtir les jalons de sa souveraineté numérique et mettre à disposition de tous les acteurs et opérateurs l'infrastructure qui accompagne la stratégie de souveraineté numérique. Un des leviers exploités par plusieurs pays (Chine, Russie, France, etc.) est d'encourager l'utilisation de logiciels « open source » que ce soient des systèmes d'exploitation en substitution au système Microsoft Windows, ou des logiciels de bureautique et autres utilisés dans les administrations. Ce type de logiciels libres jouit d'un niveau de transparence élevé, vu que leur code informatique est accessible aux développeurs et peut être personnalisé et vérifié plus facilement que des logiciels fermés. Par ailleurs, l'utilisation des logiciels « open source » permet de réduire la facture de licences d'utilisation des logiciels payants qui souvent exploitent des conditions d'utilisation ambiguës pour contrôler le traitement et stockage des données personnelles issues de leur utilisation. D'ailleurs, le développement des systèmes d'exploitation souverains les plus aboutis ont tous exploité des noyaux de systèmes « open source » comme FreeBSD (pour Kylin Chinois), Ubuntu (pour Ubuntu Kylin) ou AstraLinux (Russe) ou CLIP (Français).

3.5. Dimension Environnementale

Cette dimension est étroitement liée à la dimension technologique. En effet, le développement de « data centers » et leur mise en production requièrent beaucoup d'énergie. Cette énergie est nécessaire pour le fonctionnement des milliers de serveurs qui les composent mais aussi pour le refroidissement des CPU sans interruption. L'enjeu est donc de garantir la disponibilité de cette énergie sans interruption tout en minimisant

les émissions de CO_2 issues de sa production. Le défi est de construire et d'exploiter des « data centers » propres alimentés essentiellement par des énergies renouvelables. Par exemple, Google a tracé un objectif pour faire opérer ses data centers à l'énergie complètement dé-carbonisée d'ici 2030. La Figure 7 illustre la carte des gisements d'énergies renouvelables exploités par Google (environ 6GW d'énergie renouvelable).

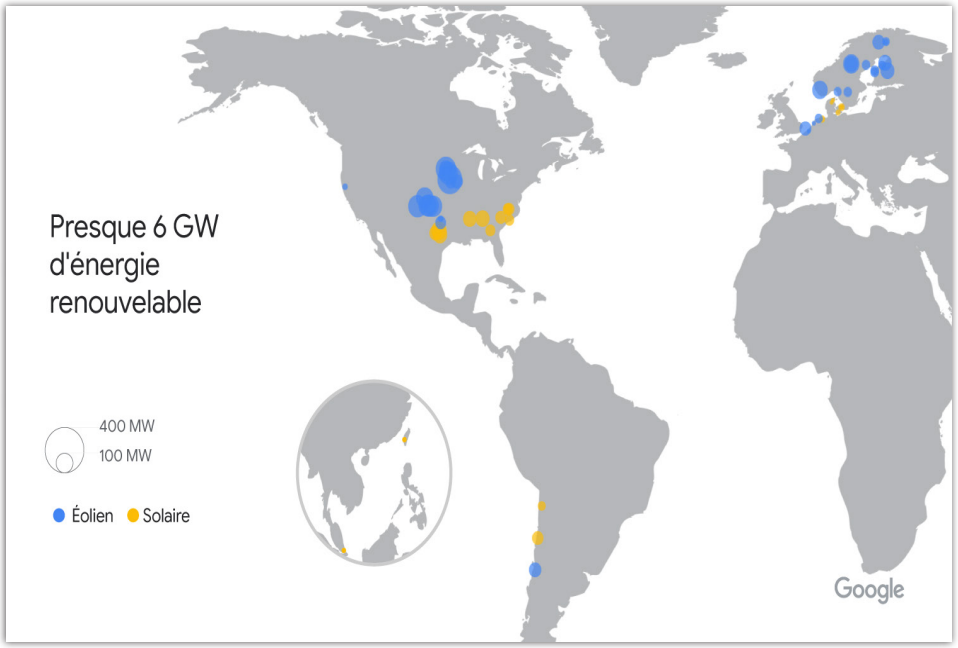

Figure 7: Carte des gisements d'énergies renouvelables de Google

L'Algérie pourrait exploiter son potentiel d'énergie solaire unique au monde pour attirer l'implantation de data centers 0 % Carbone.

3.6. Dimension Légale

L'enjeu de la dimension légale est de mettre en place le corpus juridique qui protège les citoyens et leur données personnelles et qui garantit leur autodétermination informationnelle[12]. Les expériences des pays sur ce plan sont diverses et variées. On peut en distinguer deux grandes approches[2] :

- Une approche conservatrice où l'Etat affirme son autorité non seulement sur l'infrastructure TIC du pays, mais aussi contrôle le contenu des flux de données et met en place les lois qui accompagnent leur

vision de la souveraineté numérique. Cette approche est adoptée par la Chine et la Russie, entre autres. Néanmoins, il est à noter que cette approche requière une maîtrise complète de la chaîne de valeurs des TIC : équipements de télécommunication, data centers, développement logiciels, contenus et services, et disposer d'un marché qui dépasse une masse critique qui lui permet d'être auto-suffisant même en cas de déconnexion d'Internet mondiale;

- Une approche libérale et défensive où l'Etat s'affirme à protéger les données des citoyens où elles se trouvent avec une extra-territorialité de leurs lois. C'est l'approche adoptée par l'Union européenne, la France et l'Allemagne.

Le défi est donc de tracer une trajectoire de l'évolution de l'arsenal juridique qui accompagne l'évolution de la souveraineté numérique du point de vue technologique et économique d'un pays. Placer le curseur de la régulation au bon niveau et au bon moment est un défi majeur pour construire la souveraineté numérique. A défaut, les lois promulguées ne seraient que peine perdue et lourdeur bureaucratique qui freineraient le développement du numérique dans le pays.

« Les restrictions sur la circulation des flux de données, non seulement compliquent le e-commerce, mais aussi menace de creuser les inégalités en termes de développement des TIC dans les pays en développement, ... La Chine ou l'Inde ont des marchés suffisamment grands et les capacités technologiques pour restreindre la circulation des données. … Cependant, ce n'est pas le cas de beaucoup de pays en développement. Par ailleurs, ces petits marchés s'ils adoptent une forte régulation sur les données et leur circulation risquent de faire fuir les opérateurs et perdre les bénéfices de la croissance issue des TIC»[4].

Conclusion

Le développement d'Internet durant les vingt dernières années a donné naissance à un cyberespace qui cristallise paradoxalement beaucoup d'espoirs et de craintes. C'est l'espace indéniablement le plus prospère économiquement au 21ème siècle. Cet espace promet de l'emploi et des applications au service des citoyens couvrant tous les aspects de leur quotidien: santé, agriculture, industrie, énergie, éducation, etc. Néanmoins,

certains facteurs qui ont accompagné le développement du cyberespace (vides juridiques, « laisser-faire » économique, nature transnationale des réseaux, etc.) ont permis l'émergence d'une oligarchie numérique (principalement américaine) qui détient le monopole du marché mondial du numérique. Cette oligarchie se substitue petit à petit aux missions régaliennes des Etats (monnaie virtuelle, identité numérique, service de règlement des différends, représentation diplomatique, etc.). Les services et outils mis à disposition par ces multinationales avec des visées souvent hégémoniques, sont exploités dans des actions hostiles à des Etats, gouvernement, et sociétés dans le cadre de guerres de 5ème génération. La transformation du cyberespace en un espace de conflit géopolitique a poussé plusieurs Etats et organisations transnationales à défendre leur autodétermination informationnelle sous le principe de souveraineté numérique. Cette souveraineté numérique peut prendre plusieurs formes et peut être construite graduellement en prenant en compte l'environnement politique, économique, social, technologique, environnemental et légal de chaque pays.

En somme, la souveraineté numérique est un principe fondamental né en réaction des récentes transformations du cyberespace en un espace de conflit géopolitique et domination hégémonique de certaines multinationales, le plus souvent animées par une cupidité commerciale loin de profiter aux peuples. Cette avarice met en danger des nations entières, en exploitant les données dont les usagers sont auteurs avec ou sans leur consentement, et en les mettant à disposition de parties malveillantes en vue de monter des stratégies de conflits de 5ème génération.

Dans cet article, nous avons démontré l'importance du principe de souveraineté numérique et le chemin qu'il a réussit à frayer durant les vingt dernières années à travers plusieurs expériences de pays et organisations transnationales qui défendent ce principe. Nous avons démontré également que la souveraineté numérique se construit en tenant compte des réalités politiques, économiques, technologiques, et légales de chaque pays. Le plus important est d'en prendre conscience et de tracer sa stratégie de construction de la souveraineté numérique en maîtrisant la trajectoire technologique du pays et en veillant au poids de la régulation en la matière sur l'économie ■

Références bibliographiques et webographiques

[1]. « Sovereignty », Stanford Encyclopedia of Phylosophy, https://plato.stanford.edu/entries/sovereignty/, 2020.

[2]. Pauline Türk, « Définition et enjeux de la souveraineté numérique », site d'information vie-publique.fr, https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique, 2020.

[3]. Lessig Lawrence, « Code and other laws of cyberspace », Basic Books, 2006.

[4]. Deborah Elms, « Digital Sovereignty: protectionism or autonomy? », Hinrich Foundation Report, september 2021.

[5]. Amedie, Jacob, «The Impact of Social Media on Society». Advanced Writing: Pop Culture Intersections. http://scholarcommons.scu.edu/engl_176/2. 2015.

[6]. Abbott, Daniel, « The Handbook of Fifth-Generation Warfare ». Nimble Books, 2010.

[7]. James A. Lewis, « Sovereignty and the Evolution of Internet Ideology », CSIS Center for Strategic and International Studies, october 2020.

[8]. Amaelle Guiton, « Souveraineté numérique : un modèle à inventer », Libération, 20/05/2016.

[9]. Group of Govermental Experts, « Developments in the field of information and telecommunications in the context of international security », United Nations General Assembly, 2013.

[10]. Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel. Journal Officiel de la République Algérienne Démocratique et Populaire. https://www.joradp.dz/FTP/JO-FRANCAIS/2018/F2018034.pdf

[11]. REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union. https://gdpr-info.eu/

[12]. Pauline Türk, « L'autodétermination informationnelle: un droit fondamental émergent ? », Dalloz IP/IT, N° 11, page : 616, Nov 2020.