La souveraineté numérique: Concept, enjeux et défis

Pr. Karim KHELFANE
Faculté de Droit et Sciences Politiques
Université Mouloud MAAMERI, Tizi Ouzou

Résumé

Face à la généralisation de l'usage d'Internet et son ampleur à travers le monde et face à la puissance des GAFAM et autres entreprises compétitives émergentes dans le domaine, la souveraineté des Etats se trouve plus que jamais menacée aussi bien pour les Etats développés que pour les Etats en voie de développement, d'où l'intérêt grandissant qu'ils accordent à la souveraineté numérique pour faire face à l'hégémonie des puissances numériques. Cet état de fait ouvre aussi la compétition, entre les Etats d'un coté et les entreprises de l'autre, autour d'un espace (numérique) soit à conquérir et/ou à consolider, espace intimement lié à la souveraineté nationale, d'où l'intérêt que nos institutions accordent au sujet de la souveraineté numérique.

Mots clés: souveraineté, enjeux et défis, souveraineté numérique, Internet, sécurité numérique.

ملخص

في مواجهة تعميم استخدام الأنترنت واتساع نطاقه في جميع أنحاء العالم وفي مواجة قوة الـ GAFAM والشركات المنافسة الناشئة الأخرى في هذا المجال، أصبحت سيادة الدول مهددة أكثر من أي وقت مضى سواءا بالنسبة للدول المتقدمة أو الدول النامية. ومن هنا ينبع الإهتمام المتزايد الذي يولونه للسيادة الرقمية من أجل مواجهة هيمنة القوى الرقمية. هذا الوضع يفتح المنافسة، بين الدول من جهة والشركات من جهة اخرى، حول فضاء (رقمي) يتم إكتساحه و/ أو تقويته، فضاء مرتبط إرتباطا وثيقا بالسيادة الوطنية، ومن هنا يأتي الإهتمام الذي توليه مؤسستنا لموضوع السيادة الرقمية.

الكلمات المفتاحية : السيادة، الرهانات والتحديات، السيادة الرقمية، الأنترنت، الأمن الرقمي.

Introduction

La révolution conceptuelle n'est pas neuve dans l'histoire de la souveraineté, celle-ci ayant dû plusieurs fois se remodeler, en particulier en fonction des évolutions géopolitiques, ou des mutations internationales. L'espace numérique est un enjeu de souveraineté, milieu d'une nouvelle conflictualité, espace unifié et intrinsèquement lié à toutes les activités humaines, il est devenu progressivement un enjeu de puissance tout à fait décisif dans les rapports de force, les acteurs étatiques et industriels qui en maîtrisent les ressorts conserveront l'initiative et l'indépendance et ils pourront préserver leur invulnérabilité. Inversement, ceux qui perdront le contrôle de certains compartiments de ce terrain seront réduits à agir en réaction, à dépendre d'autres acteurs hégémoniques et à subir les conséquences de leur vulnérabilité.

Alors qu'il était autrefois imaginé comme un instrument pour un «village mondial» sans frontières, Internet subit actuellement des processus complexes de renationalisation et de régionalisation. Les débats sur la régulation, le filtrage et la fragmentation du réseau marquent les origines du concept de « balkanisation » d'Internet. Celles-ci sont étroitement liées aux questions de politique et de sécurité nationale. Un Internet balkanisé est un territoire inexploré avec un système de gouvernance dans lequel les États cherchent à affirmer ou même à imposer leurs règles sur un cyberespace supervisé politiquement, techniquement et juridiquement. Cet isolement est parfois motivé par l'envie de contrôler et ou de protéger les citoyens contre du contenu dangereux. La souveraineté numérique est devenue un objectif recherché aussi bien par les puissances publiques que par les entreprises et par les citoyens. La puissance des GAFAM (Google, Apple, Facebook, Amazon et Microsoft), des NATU (Netflix, AirBnb, Tesla et Uber) ou encore des BATX (Baidu, AliBaba, Tencent et Xiaomi) en Chine remet en cause l'autorité des États sur leurs territoires, grâce à une dépendance économique crée par un quasi-monopole et la détention de données de milliards d'utilisateurs à travers le monde.

Cette contribution s'intéressera à la nouvelle forme ou au nouvel aspect de la souveraineté ainsi que les enjeux qu'elle porte à l'horizon d'une société numérique. Il s'agira d'analyser comment la notion de souveraineté numérique est utilisée pour décrire diverses formes

d'indépendance, de contrôle et d'autonomie sur les infrastructures, les technologies et les données numériques. Il est question aussi de rappeler les fondements historiques de la notion de souveraineté et ses aspects conceptuels en mettant en relief les points sur lesquels l'ère numérique conduit à une remise en question des notions traditionnelles.

Nous tenterons aussi de cerner les défis qui s'imposent aux Etats et aux différents acteurs pour la mise en œuvre de la souveraineté numérique et quelles sont les solutions à apporter au niveau national pour rétablir le contrôle et la propriété des infrastructures clés d'information et de communication, étape essentielle vers la sécurité numérique.

De Westphalie à l'ère numérique : la souveraineté des États contestée

La notion de souveraineté est définie traditionnellement[(1)] comme le pouvoir suprême exercé sur un territoire, à l'égard d'une population, par un État indépendant, libre de s'autodéterminer[(2)]. Cette notion est remise en cause, dans une société dite post-westphalienne caractérisée par l'interdépendance des États, 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 États, et se jouent des frontières physiques[(3)], mais pour autant, elle demeure toujours un élément essentiel dont découle plusieurs attributs aussi importants.

Alors que la plupart des activités humaines sont désormais régies par les technologies digitales, les États sont entrés dans un rapport de force avec les multinationales qui règnent sur les réseaux numériques. Il s'agit donc de préserver, de conquérir et/ou de reconquérir une part du pouvoir qui s'exerce dans ces nouveaux espaces, pourtant conçus pour échapper à l'emprise étatique. La maîtrise des données numériques générées par les activités de 4,5 milliards d'utilisateurs connectés, ajoutée à une situation de quasi-monopole de certaines entreprises privées surtout (GAFAM - BATX), confèrent à ces opérateurs un pouvoir qui bouleverse les modes de gouvernement.

Avec une valorisation ayant dépassé les (4100 milliards de dollars) les cinq plus grandes entreprises technologiques américaines (Google, Amazon, Facebook, Apple et Microsoft) ont symboliquement surclassé

en valorisation le PIB de l'Allemagne (3ème économie mondiale), ces entreprises (les Big Tech) sont désormais omniprésentes dans les négociations internationales, qu'il s'agisse du récent Règlement général sur la protection des données (RGPD), des accords concernant le traitement des données échangées entre l'Europe et les Etats-Unis, ou encore de la remise en cause des grands principes fiscaux, tel que l'OCDE l'envisage dans le cadre du projet BEPS (érosion de la base d'imposition et le transfert de bénéfices)(4).

À cet égard, l'héritage de la conception initiale de la souveraineté est très difficile à articuler à nos nouvelles réalités(5). Qui fixe les conditions générales d'utilisation des applications numériques ? Qui détermine les informations ou les suggestions de lectures qui doivent être adressées aux internautes sur les réseaux sociaux ? Qui conserve et exploite les données personnelles, confiées ou laissées à leur insu par les utilisateurs, dont l'agrégation forme le big data, considéré comme «le pétrole du XXIème siècle»(6)?

En effet, le développement des réseaux numériques et de l'Internet, implique que différents acteurs puissent attaquer à distance des infrastructures qui peuvent être considérées comme critiques pour le fonctionnement et la stabilité des États (usines, centrales électriques, réseaux de communication, etc.), par ailleurs, l'information se propage rapidement et ne peut plus être régulée grâce aux moyens de contrôle historiques, tels que le contrôle des frontières nationales d'un territoire(7). Or, la volonté de contrôler et d'unifier un vaste territoire composé de populations diverses est un élément constitutif de la construction historique d'un État. La diffusion incontrôlée de l'information (les textes officiels russes parlent souvent de «dissémination de l'information»), et l'accroissement de la vulnérabilité des réseaux sont donc perçus par les autorités comme une menace fondamentale pour la souveraineté et à la stabilité de la société et de l'État, d'où la nécessité d'étendre la souveraineté de l'Etat à cet espace aussi vulnérable qu'important.

Émergence de la notion de souveraineté numérique et définition(s) :

Le terme (Souveraineté numérique) apparaît au début des années 2010, sur le plan international, c'est d'abord la question du contrôle des ressources internet qui a cristallisé les inquiétudes de certains États,

désireux de limiter l'hégémonie américaine sur la gestion du réseau. Ces préoccupations sont alors d'autant plus vives que la domination historique des États-Unis s'accompagne d'une situation de quasi-monopole technique et économique des multinationales américaines(8).

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, défendent le «droit souverain» des gouvernements à «réguler le segment national de l'Internet». Les États occidentaux sont alors soucieux, avant tout, de protéger la liberté du cyberespace(9).

C'est à l'occasion de l'affaire Snowden(10) en 2013 que la donne a changé. Les révélations relatives à l'espionnage généralisé au profit des intérêts politiques et économiques américains conduisent à une remise en cause profonde du système de gouvernance des espaces numériques, notamment lors de plusieurs sommets ou forums internationaux consacrés au sujet (NETmundial de Sao Paulo en 2014, Internet Governance Forum annuels de Bali en 2013, Mexico en 2016, Paris en 2018…). Après la Chine, l'Inde et la Russie, de nombreux États, tel que le Brésil, lancent des programmes politiques industriels dédiés. 2013 marque aussi un "réveil européen" sur le sujet, l'Union européenne s'intéressant au développement de moteurs de recherche ou de systèmes d'exploitation "souverains", tout en renégociant avec les États-Unis les accords relatifs à la protection des données personnelles des utilisateurs européens.

Ainsi, si la souveraineté est un attribut de l'Etat, la souveraineté numérique est l'expression de son contrôle sur le miroir virtuel de l'économie et de la population. Ce miroir virtuel est principalement constitué des données des individus ou des institutions qui sont une ressource de plus en plus stratégique d'un point de vue économique et également un enjeu de sécurité nationale. La capacité non seulement de contrôler la captation et l'usage de ces données, mais aussi de les utiliser à des fins de progrès technologique (comme l'intelligence artificielle) est un argument de la souveraineté numérique(11).

Pour d'autres comme Florence G'sell, l'expression déroute. Elle accole deux termes qui semblent à première vue n'avoir rien à voir.

Du bas latin superanus («supérieur»), la souveraineté peut être définie, de manière générale, comme «l'attribut d'une instance telle que nul organe ne lui impose sa loi» ou, de manière plus restreinte, comme «l'attribut de l'être qui fonde l'autorité d'un État». Ainsi, le concept de «souveraineté numérique» semble reposer sur l'hypothèse que «la puissance absolue et perpétuelle» évoquée par Bodin aurait changé de visage pour correspondre, à l'époque contemporaine, à un pouvoir exercé de manière dématérialisée, au moyen d'un traitement informatisé, en réseau. Notre réalité hyperconnectée serait le lieu d'une nouvelle forme de pouvoir, portant non plus sur le territoire mais sur un univers virtuel indépendant de tout ancrage physique(12).

De son côté, le rapport de la commission française d'enquête du Sénat sur la souveraineté numérique, publié en 2019, définit la souveraineté numérique comme étant «la capacité de l'État à agir dans le cyberespace (…), condition nécessaire à la préservation de nos valeurs, (…) impliquant, d'une part, une capacité autonome d'appréciation, de décision et d'action dans le cyberespace et, d'autre part, la maîtrise de nos réseaux, nos communications électroniques et nos données»(13).

Pour les spécialistes russes de la question, le concept de cyber-souveraineté, ou souveraineté numérique provient de l'idée française de souveraineté développée par Jean Bodin (philosophe, théoricien des lois) au XVI^{ème} siècle. Cette idée renvoie au principe de la priorité du gouvernement de l'État sur son territoire : l'État étant alors considéré comme le seul garant légitime de l'intégrité de ce territoire. Ce principe implique que les autorités étatiques puissent mettre en place et faire appliquer différentes mesures, dans tous les domaines qui peuvent être considérés comme fondamentaux pour la stabilité et la sécurité de l'État (économie, éducation, etc.) sur le territoire qu'il organise. Ces mesures peuvent alors être considérées comme relevant de ses prérogatives, mais aussi comme étant des fonctions obligatoires du gouvernement de l'État. L'évolution de cette idée a conduit à la définition, au XVII^{e} siècle, des droits régaliens, puis des fonctions régaliennes(14).

Mais pour Marine Brenac, le sujet de la souveraineté numérique s'inscrit dans les débats traditionnels sur la gouvernance d'Internet et ces débats portent sur la maîtrise d'un nouvel espace, le cyberespace, dans lequel la souveraineté s'applique avec difficulté, puisque les critères classiques de son pouvoir, comme le territoire, lui font défaut(15).

Au sens étymologique, est souverain, ce ou celui qui est au-dessus de tous les autres. En cela, Dieu dans une théocratie, le roi dans une monarchie absolue ou le peuple dans une démocratie, peut être celui qui détient l'autorité suprême et autonome qualifiée de pouvoir souverain(16).

Mais selon Othmane Krari, la notion de souveraineté numérique semble antinomique. Elle juxtapose le concept de souveraineté, qui veut qu'un Etat ne soit obligé ou déterminé que par sa volonté propre, à celui du numérique qui a trait à un monde ouvert interdépendant et interconnecté. Mais la réalité pratique du numérique permet de dépasser cette contradiction conceptuelle et d'identifier les déterminants à la nécessité de disposer d'outils et de moyens technologiques souverains(17).

Même si, aujourd'hui, mise en cause par le numérique et la mondialisation, l'idée de souveraineté nationale reste fondamentalement attachée à l'ancienne notion de souveraineté politique théorisée par Locke, Voltaire, Rousseau et d'autres. Il existe toujours des prérogatives qui sont reconnues comme relevant a priori de la compétence des États. Parmi celles-ci, on admet d'abord les fonctions régaliennes : sécurité intérieure, défense, renseignement, diplomatie, justice, finances, en particulier la politique monétaire et la perception de l'impôt et des taxes(18).

Par « le numérique » nous désignons ici les sciences, technologies, usages et innovations induits par l'identification, l'étude, le stockage, la transformation, la réception ou l'émission de l'information. En effet, l'information est au centre de cette révolution scientifique, technologique et humaine, au même titre que la matière, l'énergie ou le vivant au siècle précédent. Les impacts du numérique sur notre réflexion philosophique, scientifique, technologique et sociétale transforment profondément nos sociétés contemporaines(19). Qu'en est-il de la notion de souveraineté ?

Ainsi, selon Pierre Bellanger, "la souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques". Mais aussi : "Par le cloisonnement technique et matériel du modèle de la Chine ou de l'Iran, par le moyen d'une coordination au niveau national du chiffrement des données à intérêt national, pour une nouvelle forme de contrôle de frontière "chiffré", par un système d'exploitation

en réseau faisant office de constitution, ou en insistant sur l'emplacement des applications et systèmes souverains et l'interdiction d'exportation des données[20] ". Cette vision des choses selon le même auteur, implique "l'extension de la République dans cette immatérialité informationnelle qu'est le cyberespace" et "l'expression sans entrave, sur les réseaux numériques, de la volonté collective des citoyens"[21].

La souveraineté numérique : Un nouvel espace de souveraineté à conquérir

Selon l'agence française de la sécurité des systèmes d'information (ANSSI), le cyberespace est l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées. Il est généralement caractérisé par une approche sédimentaire en trois couches[22]:

- Une première couche « physique » ou « matériel » qui regroupe les appareils d'extrémité, Cette couche dépend d'un territoire, sur lequel sont implantés les serveurs ou fermes de données ainsi que les câbles et les moyens de transmission terrestre, aérienne ou spatiale qui permettent leur connexion;

- Une deuxième couche «logicielle» regroupe les dispositifs de codage et de programmation qu'utilisent les machines (la transformation de la pensée humaine en information);

- Enfin une troisième couche "sémantique", "cognitive" ou "informationnelle" regroupe les données ou métadonnées qui sont transportées par le réseau. Un ensemble d'informations donne un message assimilable à une opinion générale ou collective constituant la dimension informationnelle du réseau.

Le cyber est également un milieu propice aux actions de propagande et de manipulation de l'information assimilables à de la subversion pour modifier l'opinion. La dimension informationnelle et les opinions qui y circulent sont aujourd'hui le support de mouvement de contestations, d'influence, de recrutement, voire l'objet de manipulation[23] où la subversion des esprits permet d'exercer la dialectique des volontés, d'affirmer ou d'imposer sa volonté sur l'autre par l'intermédiaire du «public» visé.

En effet, l'une des plus grandes problématiques auxquelles doivent faire face les États dans la course à la souveraineté numérique dans le cyberespace est que seulement quelques grandes entreprises technologiques contrôlent aujourd'hui des quantités massives de données sur leurs utilisateurs. Plus ces géants accumulent et brassent des données, plus leurs politiques et leurs actions peuvent avoir une influence considérable. Le *Cloud Act*, mis en place en mai 2018 par l'Administration Trump, rend par exemple désormais obligatoire pour les entreprises technologiques américaines la transmission de leurs données au Gouvernement dans le cadre d'une enquête, indépendamment du lieu où ces données sont stockées(24).

Dès l'arrivée du Président américain Joe Biden et suite à la nomination de la juriste et critique de la technologie Lina Khan au poste de présidente de la Commission fédérale du commerce (FTC) en mars 2021, le Président a signé le 9 juillet un décret exhortant la FTC à établir des règles sur l'utilisation de la surveillance et la collecte des données des utilisateurs par les grandes plateformes et à créer des règles «interdisant les méthodes de concurrence déloyale» qui pourraient nuire aux petites entreprises. Ce décret fait suite aux auditions du Congrès en août dernier, au cours desquelles les démocrates et les républicains ont multiplié les attaques contre les quatre PDG des grandes entreprises technologiques(25).

Pour Bernard Benhamou, depuis l'affaire Snowden, il est, désormais, inscrit dans la conscience partagée que:

- La volonté des acteurs technologiques de protéger les données de leurs usagers n'est plus un invariant économique;

- La surveillance ne concerne plus uniquement des enquêtes et des individus isolés mais l'ensemble des citoyens d'un Etat;

- Les métadonnées(26) issues de la navigation des internautes sont aussi sensibles que le contenu des échanges eux-mêmes;

- Toutes les entreprises ne disposent pas des moyens nécessaires pour protéger leurs données sensibles des intrusions issues des Etats ou d'autres acteurs économiques;

- Un Etat, par l'intrusion de ses services secrets dans l'Internet et la création de *backdoors*(27), peut prendre le risque de fragiliser à lui seul l'ensemble de l'Internet(28).

Il faut noter aussi que l'absence de facteurs déterminants comme le temps et la distance au sein du cyberespace amplifie la notion de brouillard d'une guerre numérique ou cyber guerre. Son opacité permet le retour de modes d'action directs dont les seuils d'acceptation sont plus bas que les opérations militaires conventionnelles. Il permet un retour à moindre frais de l'offensive asymétrique ou hybride, en réduisant les écarts de puissance entre les différents acteurs, voire en complément d'actions conventionnelles, tout en permettant à son auteur de se dissimuler au sein de la toile par écrans interposés. Les conflictualités dans le cyber peuvent être caractérisées par une ou plusieurs combinaisons d'actions de recherche d'informations (cyberespionnage), d'actions de perturbation, de destruction ou de prise de contrôle à distance de systèmes informatiques (cyberattaque).

La caractérisation de l'agresseur lui-même révèle une typologie plus large que dans les conflits classiques. Les auteurs peuvent être des Etats, des organisations internationales ou nationales, des entreprises, des organisations criminelles ou terroristes, mais également des individus (militants, lanceurs d'alerte, *hackers*) qui peuvent déclencher une crise en quelques instants avec un Smartphone. Sur ce dernier point réside la singularité du cyber sur les autres milieux, avec l'émergence de l'individu comme acteur direct. Ainsi, il existe une spécificité propre à la cyber conflictualité au travers de ses caractéristiques intrinsèques, l'extraterritorialité de son champ d'action et la multiplicité de ses acteurs(29).

Les points de vue opposés sur les Big Tech et sur la légitimité de l'État à lutter contre leur influence, et contre leur pouvoir de marché, recoupent une divergence philosophique portant sur ce que recouvre la notion même de liberté. Tandis que dans une perspective libérale la liberté est l'absence de contrainte, dans la tradition républicaine elle est insuffisante pour assurer la liberté de l'homme, qui suppose l'absence de domination et d'arbitraire. Dans ce sens, on peut légitimement parler aujourd'hui de «féodalités numériques», par égard au pouvoir arbitraire dont disposent les plateformes, et à leurs tentatives de reprendre à leurs compte certains des attributs de la souveraineté, tel que l'émission de monnaie(30).

Conquérir et consolider la souveraineté numérique : un enjeu de taille pour l'Algérie

Au moment où le "cyber" est devenu un domaine de souveraineté nationale et sous régionale à protéger et à défendre au même titre que les domaines terrestre, maritime, spatial et aérien; alors que lors du Sommet de Juillet 2016 à Varsovie, en Pologne, l'OTAN a acté le cyberespace comme "terrain d'opérations militaires"; à l'aune de la cyber guerre, du cyber espionnage politico-économique, de la campagne de désinformation et de déstabilisation, du sabotage industriel ou autres cyber menaces à la sécurité nationale et à l'intégrité du cyberespace des États, avec les agences de renseignement qui rivalisent d'adresse: c'est par le prisme d'une stratégie de cyberdéfense forte qu'on peut aujourd'hui appréhender les conséquences ravageuses et l'impact de ces menaces sur le plan politique, social, économique et militaire(31).

Pour ce qui est du continent africain, d'après le rapport GCI 2017, rendu public à la suite de l'étude réalisée par l'Union Internationale des Télécommunications (UIT) sur les évolutions en cybersécurité, plusieurs pays ont mis en place de bonnes pratiques de renforcement des capacités de lutte contre la cybercriminalité. Cet effort est appréciable à travers l'évolution du positionnement des pays africains dans le classement mondial des pays dont l'indice de cybersécurité, qui mesure le niveau de développement de chaque pays est remarquable(32).

La *Global Cybersecurity Index* mesure l'engagement et les mesures prises par les États pour améliorer la cybersécurité. Cette mesure consiste à faire une cartographie des réponses à 82 questions qui couvrent cinq piliers que sont : les mesures légales, les mesures techniques, les mesures organisationnelles, les mesures de développement de capacité et les mesures de coopération. Pour l'édition 2020, les données de 194 États ont été prises en compte dont 43 pays africains. On notera que parmi les pays africains les mieux classés, figurent respectivement : Ile Maurice première en Afrique (17ème au rang mondial), Tanzanie en seconde position (37ème au rang mondial), Ghana en troisième

position (43ème au rang mondial), Nigéria en quatrième position, puis le Benin. Notre voisin la Tunisie est classée (45ème au rang mondial).

A l'instar des autres pays en voie de développement, l'Algérie, par le biais du représentant de son gouvernement Mustapha ABBANI, au sujet des conclusions du rapport du Groupe d'experts gouvernementaux sur les technologies de l'information et des télécommunications, a insisté sur le besoin d'établir des normes de transparence et de confiance pour mieux encadrer les usages des technologies et les télécommunications à des fins pacifiques et de développement. Au passage, il a signalé qu'en Algérie une démarche d'ensemble pour lutter contre la cybercriminalité et mieux comprendre les défis en ce domaine avait été mise au point. Il a en outre appelé à l'amélioration de la coordination interétatique des actions de prévention et de lutte contre la cybercriminalité «qui appuie l'activité d'entités terroristes» tout en plaidant pour la conclusion d'un accord pour lutter contre les crimes numériques touchant les États et les individus(34).

Sur le plan normatif, la loi 18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel(35) apporte une précision dans son article 3 au sujet de la définition des «Données à caractère personnel». «Aux fins de la présente loi, on entend par : «Données à caractère personnel» : toute information, quel qu'en soit son support, concernant une personne identifiée ou identifiable, ci-dessous dénommée «personne concernée», d'une manière directe ou indirecte, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, biométrique, psychique, économique, culturelle ou sociale ».

La loi veille aussi a ce que le traitement des données à caractère personnel, quelle que soit son origine ou sa forme, se fasse dans le cadre du respect de la dignité humaine, de la vie privée, des libertés publiques et ne doit pas porter atteinte aux droits des personnes, à leur honneur et à leur réputation(36). Quant au traitement des données à caractère personnel, il ne peut être effectué qu'avec le consentement expresse de la personne concernée(37).

Pour assurer l'application des dispositions énoncées dans la loi, celle-ci n'a pas manqué de prévoir un organe chargé de leurs mise en

œuvre. Ainsi, le titre III de la loi traite de l'Autorité nationale de protection des données à caractère personnel[38], organe qui a été créé en Aout 2022.

L'objectif principal de l'Autorité nationale est de veiller à ce que le traitement des données à caractère personnel soit mis en œuvre, conformément aux dispositions de la présente loi et de s'assurer que l'utilisation des technologies de l'information et de la communication ne comporte pas de menaces au regard des droits des personnes, des libertés publiques et de la vie privée[39].

Selon Cherif Bencharef, même si cette loi reste incomplète par rapport au règlement général sur la protection des données, elle est un point de départ vers une prise de conscience en ce qui concerne la nécessité de protéger la vie privée et l'établissement des normes relatives à la protection des données en Algérie (…) En accordant aux personnes physiques de nouveaux droits et en établissant les règles relatives au traitement de ces données, la loi donne à chaque algérien la maitrise des informations qui le concerne et par extension établit les règles relatives au respect de la vie privée[40].

A ce titre, il faut noter que l'article 47 de la Constitution (2020) stipule : « Toute personne a droit à la protection de sa vie privée et de son honneur. Toute personne a droit au secret de sa correspondance et de ses communications privées, sous toutes leurs formes. Aucune atteinte aux droits cités aux paragraphes 1er et 2 n'est permise sans une décision motivée de l'autorité judiciaire. La protection des personnes dans le traitement des données à caractère personnel est un droit fondamental. La loi punit toute violation des droits sus-mentionnés»[41].

A cet effet, le plan d'action du Gouvernement adopté tout récemment en septembre 2021, s'est engagé à poursuivre l'adaptation du cadre normatif et organisationnel nécessaire à la transformation numérique en mettant l'accent sur l'accélération de l'utilisation de la certification électronique, comme préalable à la signature électronique des documents. Par ailleurs et pour garantir une cohérence d'ensemble, une efficacité et rationalité dans ce domaine, le Gouvernement procédera, notamment (entre autres) :

- À la mutualisation des ressources et la mise en cohérence

des plans de développement sectoriels de numérisation ainsi que la mise en place des mécanismes d'interopérabilité entre les différentes administrations ;

- La production de contenus numériques nationaux de qualité, pour assurer la souveraineté en la matière ;

- Le renforcement des moyens nécessaires à la sécurisation des systèmes d'information et au développement de solutions de cyber sécurité(42).

Dans l'ensemble des dispositions, d'activités et de projets mis en branle par notre Gouvernant pour développer le secteur de l'économie numérique et accompagner la transformation de notre société, la souveraineté numérique commence à occuper, à juste titre, une place de plus en plus importante. Car, malgré le niveau de développement plutôt relatif qu'on a en ce moment dans le secteur du digital(43), le nombre de cyber-crimes va grandissant, voire galopant. Cela va sans dire, puisqu'il est désormais établi que ce n'est pas l'expansion du cyberespace qui crée de nouveaux crimes, mais des criminels qui s'adaptent très rapidement aux nouveaux outils mis à leur disposition(44).

Pour faire face à toutes ces menaces et cette nouvelle forme de criminalité et les différentes menaces à la souveraineté du pays et sa propre sécurité, le Gouvernement algérien recours au blocage de certains sites et réseaux sociaux étrangers, et met progressivement en place un ensemble de mesures sous forme de lois (une réforme du code pénal adoptée en avril 2020), d'organisations spécialisées (ex. Autorité de régulation de la poste et des communications électroniques) et même d'infrastructures pouvant assurer la protection numérique du grand public (instituions étatiques, entreprises et citoyens), l'Algérie a ainsi promulgué plusieurs lois portant sur la cybersécurité(45), la lutte contre la cybercriminalité, la lutte contre la haine sur Internet,…etc.

A cet effet, et pour apporter des solutions efficaces et effectives sur le terrain et compte tenu de la gravité des crimes de l'espace virtuel, le Ministère de la Communication a placé la participation à l'effort visant la lutte contre la cybercriminalité parmi les priorités de son programme d'action. La première mesure consistait en la mise en place d'un cadre juridique approprié et ce par la promulgation d'un décret exécutif définissant les modalités d'exercice des activités médiatiques via Internet, en sus de l'activation de ce décret requérant l'hébergement des sites électroniques dans le domaine DZ(46).

Tout en rappelant les risques qui pèsent sur la sécurité du pays du fait de l'activité criminelle à travers le cyberespace[47], il a notamment affirmé que "Notre pays est conscient des défis imposés par le mauvais usage d'Internet, c'est pourquoi il veille à garantir la sécurité informatique relative à la vie des individus et l'intégrité des organes de l'Etat", notamment par "la mise en place d'un contenu purement national et de lois idoines, outre la création d'entreprises spécialisées", comme la création du premier Centre de cybersécurité qui permet à plusieurs entreprises et organes de bénéficier de ses services à même de faire face aux cyber-attaques. "Le Ministre a par ailleurs affirmé sa détermination à défendre sa souveraineté numérique nationale et à protéger le peuple de tous les plans et activités destructeurs, impliquant des contenus diffusés sur les réseaux sociaux, considérés comme une arme dirigée contre les peuples et les pays selon les intérêts des lobbies hostiles et ceux qui les soutiennent"[48].

C'est là un défi majeur, permanent, pour les pouvoirs publics algériens au regard de la diversité et de la taille du pays que de contrôler et réguler l'espace numérique et l'éloigner des usages malveillants qui peuvent nuire à la société en général et à la sécurité du pays de manière particulière, car veiller à la souveraineté numérique ne consiste pas à "isoler" l'Algérie du reste du monde, mais plutôt à défendre l'intérêt stratégique de l'État et développer sa propre capacité numérique.

Pour l'expert Mohamed Cherif Amokrane, tout reste à faire en matière de souveraineté numérique. Un grand paradoxe réside dans le fait que plus nous investissons dans l'infrastructure et le matériel technologique, et plus nous cédons de territoires numériques. Car lorsque l'internaute algérien s'équipe en connexion internet, il l'utilise pour rendre les Google, Facebook, Youtube, Apple, Microsoft…toujours plus forts. Continuellement, ces mastodontes élargissent l'écart par rapport à nous, ils connaissent de plus en plus notre peuple et utilisent leurs «butins» dans les domaines économique, politique, social et culturel[49].

Selon ce même expert, deux projets doivent être construits en parallèle : d'un côté, l'accès aux nouvelles technologies, les pouvoirs publics et les opérateurs économiques y travaillent déjà, de l'autre, une politique de performance, c'est l'enjeu d'un futur pas aussi lointain qu'on pourrait s'imaginer. Ceci étant dit, il faut mettre en garde contre une erreur fatale : confier la mission de la performance uniquement aux

pouvoirs publics. Si les USA sont aujourd'hui la plus grande puissance numérique au monde, c'est avant tout grâce à des startups devenues plus fortes que certains Etats développés(50).

De son côté, Mustapha Zerouali expert en stratégie numérique suggère que "se prémunir des piratages est difficile de nos jours, au vu des *backdoors* installés, souvent par les fournisseurs des services digitaux et les éditeurs des applications utilisant les tiers. Mais il y a des minima lorsqu'il s'agit des entités officielles. Disposer d'une armée de spécialistes de SSI est comme disposer d'une branche ou d'un corps spécialisé de l'ANP. Selon lui, il faudra anticiper en disposant de serveur en local (supports connus, paramétrés et déconnectables en cas de faille)"(51).

Aussi, pour cet expert, les meilleures alternatives qui s'offrent à nous consistent à construire des applications et des solutions domestiques et locales avec des ingénieurs nationaux et des solutions de sécurité nationales, comme en Russie, en Chine, en Inde et au Brésil. Cette solution permet de se déconnecter d'internet en cas de menaces extérieures systémiques sans remettre en cause les flux et les services nationaux(52).

Conclusion

Les nations du monde entier tentent de s'approprier les avantages -tant économiques que géopolitiques- qui découlent de l'évolution rapide des technologies du numérique. Savoir à qui appartiennent les technologies de l'avenir, qui les produit, et qui en fixe les normes et réglemente leur utilisation devient ainsi un élément inévitable de la compétition géopolitique.

A cet effet, certains proposent deux models possibles d'être souverain, Le premier implique l'indépendance complète des entreprises et institutions publiques algériennes vis-à-vis des services et infrastructures étrangers. Viser ce modèle de souveraineté nécessiterait d'exclure les acteurs étrangers du marché algérien et de reconstruire de fond en comble les infrastructures numériques. Le second encourage la reconnaissance des dépendances entre les acteurs étrangers et algériens tout en valorisant les compétences propres de l'État et en préservant sa liberté de choix et l'intérêt national. Dans ce modèle, l'objectif est de

s'assurer que les services existants puissent être utilisés au profit de l'Algérie afin de favoriser le développement économique et la liberté des échanges.

Pour réussir avec le deuxième modèle, certaines priorités doivent être prises en charge et qui répondent aux défis majeurs que rencontre notre pays dans le domaine:

1. Accélérer la numérisation de l'économie et de l'administration algériennes(53), afin d'augmenter la demande en services, ainsi que le développement de services (Business to Business) natifs du Cloud, qui seront la principale source de valeur dans les années à venir (économie numérique puissante);
2. Créer un processus pour identifier les domaines qui posent d'importantes questions de souveraineté et qui devraient être priorisés;
3. La revendication de souveraineté numérique s'accompagne souvent d'une perspective techno-nationaliste, qui entend accroître la puissance de l'État par le biais d'une plus grande maîtrise de l'innovation, et des industries de pointe. Pour faire advenir cette vision, il est alors souhaitable de mettre en œuvre des politiques de soutien ciblées, ainsi que des mesures protectionnistes visant à faire émerger de grandes plateformes algériennes;
4. L'élaboration d'une stratégie nationale spécifique au numérique formaliserait le développement de facteurs de souveraineté étatique, qui seront aussi des facteurs de puissance au sein des trois couches du cyberespace (une feuille de route définissant un cadre réglementaire et financier et des objectifs dans les trois couches du cyberespace). Le développement d'un dispositif d'intelligence économique axé sur l'économie numérique est un impératif qui serait également l'un des objectifs de la stratégie nationale;
5. La création d'un conseil national de recherche sur le numérique(54) centré sur le monde académique, son action compléterait les champs de réflexion d'un conseil national du numérique centré sur les élus, la société civile et le monde économique. Ces conseils devaient préparer la maîtrise et la pérennité des facteurs clés nationaux d'une souveraineté pour préparer la prochaine étape de la révolution numérique en marche;

6. Le rétablissement d'un contrôle démocratique en matière de numérique requiert donc la reconnaissance de la compétence de la puissance publique sur son « territoire numérique ». Mais les frontières de ce dernier sont encore imprécises. Dans une telle situation, la coopération entre États peut s'avérer nécessaire pour atteindre notre objectif.

Il faudra aussi renforcer les capacités nationales de cybersécurité et veiller à l'adaptation continue du cadre légal et réglementaire ainsi que le renforcement de la lutte contre la cybercriminalité. La formation et la sensibilisation sont aussi des mesures à encourager et à généraliser pour la construction d'une culture numérique au service de l'économie, du commerce, de la défense et de la sécurité.

Aussi, et comme nous le rappelle si bien Othmane Krari[55], l'avantage technologique américain, ou même tout autre, n'est pas absolu telle que l'illustre la domination d'acteurs chinois sur la technologie 5G.

Aussi, et à défaut d'un *cyberpower* à l'américaine, et pour atteindre le seuil minimal d'une souveraineté partielle à l'image de certains pays, il est plus qu'urgent de penser la nécessité d'une veille stratégique permanente dans un espace numérique en mutation constante, car il n'existe pas de souveraineté absolue. C'est un idéal à atteindre mais qui nécessite des efforts à plusieurs niveaux, comme offrir un *Cloud* souverain à l'Algérie et lister les domaines technologiques sur lesquels il souhaite disposer d'outils souverains[56].

Enfin, derrière les enjeux de la souveraineté numérique «se posent ceux de la résilience de nos sociétés. Dans cette perspective, le plus urgent demeure sans doute de réinjecter de l'humain dans le réel, au moins autant que du souverain dans le virtuel. Internet ne mérite pas de majuscule : sans nous, la toile n'est qu'un amas de câbles»[57]■

Références

1. En 1648 les nations européennes signaient le traité de Westphalie. Véritable genèse de la diplomatie et du droit international, il reconnait la supériorité de l'Etat sur le territoire. L'Europe devient alors un ensemble d'Etats, disposant de frontières précises et reconnues, et dont la souveraineté doit être respectée. Il induit qu'il n'existe pas d'autres souverainetés que celle de l'Etat.

2. Voir l'apport à ce concept juridique de Jean Bodin et Charles Loyseau, au XVI^{ème} siècle puis de Louis le Fur et Raymond Carré de Malberg au XX^{ème} siècle.

3. Pauline Türk, Définition et enjeux de la souveraineté numérique, université Côte d'Azur, www.vie-publique.fr, publiée le 14/9/2020.

4. Gilles Babinet, La fin de l'Etat-nation ? Partie 1, les glissements de souveraineté induits par la technologie, Institut Montaigne. Publié le 12/11/2018 sur www.institutmontaigne.org .

5. Thierry Ménissier, Les formes imparfaites de la souveraineté numérique, séminaire «Société & souveraineté», Grenoble, 2020.

6. Pauline Türk, Définition et enjeux de la souveraineté numérique.

7. Voir Bertrand Boyer, Guérilla 2.0, Guerres irrégulières dans le cyberespace, préface du général d'armée Thierry Burkhard, éditions de l'École De Guerre, collection «Ligne De Front », 2020.

8. «L'internet était à nous», affirmait Barack Obama dans une interview au site Recode. « Nos entreprises l'ont créé, étendu et perfectionné de telle façon que la concurrence ne peut pas suivre ».

9. Bernard Benhamou, La gouvernance de l'internet après Snowden, la Politique étrangère, 2014.

10. France Culture le présente ainsi : « En 2013, âgé alors de 29 ans, Edouard Snowden, ancien employé de la CIA et de la NSA, permettait au monde entier de découvrir avec quel entrain les agences de renseignement américaines et leurs partenaires s'adonnaient à la surveillance de masse ». In : https://www.franceculture.fr/emissions/lactualite-des-industries-culturelles-et-du-numerique/lactualite-des-industries-culturelles-et-du-numerique-du-dimanche-22-septembre-2019.

11. Sarah Guillo, La Souveraineté numérique française passera par l'investissement dans les technologies numériques, Science Pochaire Digital, Gouvernance et Souveraineté, p3.

12. Florence G'sell, Qu'est-ce que la souveraineté numérique ? in, https://www.sciencespo.fr/public/chaire-numerique/2020/07/09/quest-ce-que-la-souveraineté-numerique/ 9 juillet 2020, p. 01.

13. Institut Inria, Souveraineté numérique : Quel rôle pour la recherche ?, in : https://www.inria.fr/fr/souverainete-numerique-role-recherche, 29 mars 2021 lis à jour le 13 juillet 2021.

14. Marie-Gabrielle Bertran, La recherche d'une souveraineté numérique en Russie : à qui profite-t-elle ?, la revue géopolitique, publié le13/6/2021, www.diploweb.com

15. Marine Brenac, La souveraineté numérique sur les données personnelles Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique, Maitrise en droit, Univérsité Laval, Québec, Canada, 2017, p. 01.

16. Jean-Gabriel Ganascia, Eric Germain, Claude Kirchner, La souveraineté à l'ère du numérique. Reste maitres de nos choix et de nos valeurs, CERNA Edition provisoire, 27 mai 2018. p.7.

17. Souveraineté numérique : Quatre questions à Othmane Krari, In : https://www.cmais-strat.com , 16-10-2020.

18. Op. Cit. p. 10.

19. Othmane Krari, Op. Cit. p.13.

20. Idem. p. 16.

21. Cité in, Pauline Türk, Définition et enjeux de la souveraineté numérique, https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique , p.5.

22. Christophe Gasançon, Le cyberespace, nouvel espace de souveraineté à conquérir, Centre des Hautes Etudes Militaires, France, publié le 22/5/2018, www.geostrategia.fr

23. Voir: The PerfectWeapon: How Russian Cyberpower Invaded the U.S, The New York Times, 2016. www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

24. Souveraineté numérique : quel rôle pour la recherche ?, Institut français de recherche en sciences et technologies du numérique, publié le 21/3/2021 in: www.inria.fr

25. Pourquoi la guerre de Biden contre Big Tech est malavisée, article traduit de Forbes US par Steve Denning, 28 juillet 2021, In : https://www.forbes.fr/technologie/adr-pourquoi-la-guerre-de-biden-contre-big-tech-est-malavisee/

26. Une métadonnée est une caractéristique formelle normalisée et structurée utilisée pour la description et le traitement des contenus des ressources numériques. Dictionnaire Le Robert.

27. Un backdoor, mot anglais qui se traduit en français par « porte dérobée » ou «trappe», est un cheval de Troie caché dans un logiciel, un service en ligne ou un système informatique entier et dont l'utilisateur n'a pas connaissance. In : https://www.futura-sciences.com/tech/definitions/informatique-backdoor-2047/

28. Cité in, Laure de la Raudière, Op. Cit. A noter au passage que ces révélations d'Edward Snowden semblent avoir déjà engendré d'importants changements comportementaux. Selon une étude du Pew Research Center en 2013, 86% des internautes « ont déjà tenté de détruire ou de dissimuler leurs informations numériques » et 55% « ont cherché à éviter d'être observés en ligne par leur employeur ou par les instances gouvernementales ». Idem.

29. Christophe Gasançon, Le cyberespace, nouvel espace de souveraineté à conquérir, Op. Cit.

30. Christophe Gasançon, Op. Cit.

31. Francois-Xavier Djimgou, Souveraineté numérique et cyberdéfense : un enjeu de taille pour l'Afrique, Edilivre, 26 juin 2019. https://www.linkedin.com/pulse/souverainet%C3%A9-num%C3%A9rique-et-cyberd%C3%A9fense-un-enjeu-de-djimgou-cissp-

32. Ammar Belhimer, Le scandale Pegasus est une preuve de plus que nul n'est à l'abri de la cybercriminalité, Radio Algérienne, https://www.radioalgerie.dz.

33. Pour plus de détails sur le classement Etat par Etat en Afrique et à travers le monde, voir : Global Cybersecurity Index : Classement des pays africains en 2020. In : https://cybersecuritymag.africa/global-cybersecurity-index-2020-classement-pays-africains

34. Assemblée générale, Première commission, Soixante-douzième session, 19ème et 20ème Séance, Le cyberespace, « nouvelle frontière de la sécurité stratégique », au cœur des préoccupations de la Première Commission, (AG/DSI/3586) du 23 Octobre 2017. In : https ://www.un.org/press/fr/2017/AGDSI3586.doc.htm

35. Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel, JORA n° 34 du 10 juin 2018.

36. Article 02 de la loi 18-07.

37. Article 7 de la loi 18-07.

38. Voir les articles de 22 à 31 de la loi 18-07. L'Article 22 stipule : « Il est créé, auprès du Président de la République, une autorité administrative indépendante de protection des données à caractère personnel, désignée ci-après « l'autorité nationale», dont le siège est fixé à Alger. L'autorité nationale jouit de la personnalité morale et de l'autonomie financière et administrative ».

39. Article 25 de la loi 18-07.

40. Cherif Bencharef, De la nécessité pour les algériens de protéger leurs données personnelles, in : https://www.elwatan.com/edition/contributions/616170-03-11-2019 03 Novembre 2019.

41. Décret présidentiel n° 20-442 du 30-12-2020 relatif à la promulgation au journal officiel de la République algérienne démocratique et populaire de la révision constitutionnelle adoptée par référendum le 1er novembre 2020. JORA n°82 du 30-12-2020.

42. Voir, Plan d'action du Gouvernement pour la mise en œuvre du Programme du Président de la République. Septembre 2021. In : http://www.apn.dz/fr/images/actualits_specials_3/plan-d-action-du-gouvernement-2021-fr.pdf p.20.

43. Selon l'APS, qui cite le dernier rapport du site web datareportal spécialisé dans les statistiques relatives à l´internet fixe et mobile dans le monde, au 31 janvier 2021,

l´Algérie comptait 26,35 millions d'utilisateurs internet ce qui représente une hausse de 3,6 millions (16%) depuis janvier 2020. Ce chiffre représente le nombre d'utilisateurs effectifs d'internet et non le nombre d'abonnés à internet en Algérie qui était de 41,8 millions au troisième trimestre de 2020, selon le dernier rapport de l'Autorité de Régulation de la Poste et des communications électroniques (ARPCE). Aussi, le taux de pénétration d'Internet en Algérie était de 59,6% en janvier 2021, sur une population estimée à 44,23 millions (source Onu). Le nombre d'utilisateurs de médias sociaux (Facebook, Youtube, Instagram, Tweeter, etc.) en Algérie a également connu une évolution au 31 janvier 2021. Quelque 3 millions de nouveaux utilisateurs de médias sociaux ont été enregistrés, soit une augmentation de 13,6% en une année, portant ainsi le nombre total d'utilisateurs de ces applications à 25 millions, soit 56,5% de la population totale. Voir, APS, Le nombre d'internautes a augmenté de 3,6 millions en une année, 27-02-2021, In : https://www.aps.dz/sante-science-technologie/117728-algerie-le-nombre-d-internautes-a-augmente-de-3-6-millions-en-une-annee .

44. A titre d'exemple, le Ministre de la Communication, Amar Belhimer signale au passage que : « Le Makhzen marocain mène actuellement une guerre médiatique et électronique contre tout ce qui est algérien en diffusant de fausses informations, la démarche agressive du royaume marocain, allié de l'entité sioniste s'est appuyée sur une technologie de pointe à l'aide d'un logiciel d'espionnage appelé Pegasus. « Ce scandale d'espionnage israélo-marocain est une preuve de plus que nul n'est à l'abri de la cybercriminalité dont les auteurs sont des individus ou des parties sans scrupules ». L'Algérie déterminée à défendre sa souveraineté numérique, Publié le : 12/8/ 2021 sur www.aps.dz

45. La cybersécurité est un concept regroupant les éléments ayant pour objectif la protection des systèmes informatiques (système, réseau, programme) et leurs données. Ces moyens de protection sont multiples et de plusieurs types : technique (ex. Firewall, antivirus…) ; conceptuel (méthode de gestion des risques Ebios...) ; humain (ingénieur sécurité, formation, compétences) ; législatif (organisme d'État, normes ISO, etc.).

46. Décret Exécutif 20-332 du 22 novembre 2020 fixant les modalités de l'activité d'information en ligne et la diffusion de mise au point ou rectification sur le site électronique. JORA n° 70 du 25 novembre 2020.

47. Selon le Ministre, l'Algérie a occupé la 1ère place arabe et la 14ème mondiale sur la liste des pays les plus exposés à la cybercriminalité pour l'année 2018, le Ministre a affirmé que plus de 80 sites étrangers mènent des campagnes de diffamation contre l'Algérie.

48. L'Algérie déterminée à défendre sa souveraineté numérique, publié le 12/8/2021 sur www.aps.dz

49. Mohamed cherif Amokrane, Op. Cit.

50. Ibid.

51. Mustapha Zerouali, Il faut défendre notre sécurité et souveraineté numériques, https://www.lexpression.dz , du 28-10-2021.

52. Mustapha Zerouali,Op. Cit.

53. Au sujet de cet important défi, voir la contribution d'Abderrahmane Benkhalfa, Digitalisation de l'économie. Cohérence, pragmatisme et ciblage, Revue IFIDard, Numéro 4/ 1er semestre 2020, numéro consacré à la transformation numérique en Algérie : Acquis et défis. Pp. 7-8.

54. Pour Ludovic Mé, adjoint au directeur scientifique en charge du domaine de recherche "Cybersécurité" chez Inria (centre de recherche en France), la solution pour viser une véritable souveraineté numérique serait de pouvoir maitriser toute la chaîne, du processeur au service : « sans maitriser toute cette chaîne, dans les faits, on ne maîtrise rien ».

55. Souveraineté numérique : Quatre questions à Othmane Krari, In : https://www.cmais-strat.com , 16-10-2020, l'italique est de nous.

56. Grégoire Germain, Paul Massart, Op. Cit. p. 56.

57. Caroline Richemont, Eddy Maaroufi, Veille M3 : La souveraineté numérique, oui, mais laquelle ? 19-5-2012. In : https://www.millenaire3.com