

# Révolution numérique et enjeux de souveraineté : apprendre à penser global



**Alix DESFORGES**

*Docteure de l'Institut Français de Géopolitique*

*Chercheuse Post Doctorante*

*GEODE - Université Paris 8*

Les appels politiques à construire une « souveraineté numérique » en France mais aussi en Europe se sont multipliés ces dernières années. En décembre 2019, Jean-Yves le Drian, Ministre des Affaires Étrangères, appelait à « construire une souveraineté numérique européenne ». Le 1er mars dernier, les chefs de gouvernement de l'Allemagne, du Danemark, de l'Estonie et de la Finlande menaient une initiative conjointe inédite. Dans une lettre adressée à la présidente de la commission européenne, ils estiment qu'« *il est désormais l'heure pour l'Europe d'être numériquement souveraine* » et enjoignent la Commission à agir pour « *exploiter les atouts [de l'Union Européenne] et réduire [ses] faiblesses stratégiques* »<sup>1</sup>.

La révolution numérique vient bouleverser les modalités de l'exercice de la souveraineté des États parce qu'elle permet des activités transfrontières et mais aussi parce qu'elle offre des moyens d'actions à

distance pour espionner et saboter des réseaux en dissimulant son identité et s'abritant derrière des juridictions multiples.

## **Une volonté politique transformée en solutions techniques**

Loin de n'être que des mots, de nombreuses initiatives ont été lancées depuis plusieurs années par les États dont la France. Ces initiatives se formalisent essentiellement par deux types d'actions. Tout d'abord, le soutien à la mise en œuvre d'initiatives industrielles pour favoriser l'émergence de solutions techniques et plus généralement à la constitution de filières industrielles nationales et européennes. La France fait même figure de précurseur en Europe avec son initiative malheureuse de *cloud* souverain lancée en 2010. Le deuxième type d'actions est le recours à la voix normative, réglementaire et légale – ce qui influence également à la structuration du marché.

En France, si les toutes premières initiatives étaient surtout portées par des arguments de nature économique et industrielle (plan de relance), dès le début des années 2010, l'argument sécuritaire vient alimenter les discours militant en faveur d'une souveraineté numérique et pour devenir même un argument central. L'exemple du *cloud* est particulièrement symptomatique de cette évolution discursive. Mais surtout, d'un objet technique et mode d'organisation d'un système d'information, le *cloud* est devenu au fil des années un objet politique, géopolitique et stratégique au regard des enjeux de souveraineté et de puissance qu'il soulève.<sup>2</sup>

## **D'une approche économique et technique aux enjeux stratégiques**

Alors qu'à l'origine, les principaux débats politiques sur la souveraineté numérique portaient d'abord sur des problématiques économiques et sécuritaires, le concept a aujourd'hui largement dépassé ces seules préoccupations pour revêtir une dimension stratégique multidimensionnelle. Ainsi, la question des données et les oligopoles américains ou chinois deviennent des enjeux discutés. Les États européens dont la France s'inquiètent de la situation de domination du marché par quelques entreprises non européennes et mettent en œuvre des stratégies (en ordre plus ou moins dispersé) pour faire émerger des entreprises européennes susceptibles de les concurrencer. Face à un cyberespionnage qui ne connaît pas la crise y compris entre alliés et la manipulation des données personnelles et des informations sur les grandes plate-formes, les États européens ont pris conscience qu'ils ne pouvaient pas se fier aux technologies et services numériques étrangers. Cette défiance bénéficie aux discours prônant une « souveraineté numérique européenne » en s'appuyant sur le développement de capacités technologiques et de services numériques au sein des États-membres de l'UE. Ces discours se font d'autant plus forts lorsque cette dépendance touche à des capacités souveraines des États notamment dans le domaine militaire et dans celui du renseignement. Il s'agit bien sûr de saisir des opportunités économiques (participation à un marché en pleine expansion) et de d'assurer la sécurité des produits et services notamment par la protection des données, mais aussi de pallier les effets stratégiques d'une telle situation.

En effet, plusieurs événements (dont les affaires Snowden et Cambridge Analytica) ont joué un rôle de catalyseur dans la prise de conscience des risques géopolitiques induits par la situation de dépendance européenne vis-à-vis d'entreprises du numérique étrangères : déstabilisation politique, espionnage stratégique et économique etc. Autant de menaces

pour l'avenir politique, économique et démocratique de l'Union Européenne et de ses États membres renforcées par un contexte géopolitique particulièrement tendu (élection de Donald Trump aux États-Unis, Brexit, déstabilisations russes aux frontières est de l'Europe).

En outre, avec l'interconnexion globale des systèmes d'information et de communication, des pans entiers des activités humaines sont transformés en données numériques, et celles-ci se retrouvent de plus en plus au cœur des processus de décision économique, politique, militaire etc. Les données numériques sont également utilisées pour résoudre des problèmes de plus en plus complexes auxquels le monde d'aujourd'hui doit faire face tel que le changement climatique ou la lutte contre la covid-19. La compréhension de leurs impacts sociaux et politiques est d'autant plus essentielle que deux ruptures technologiques majeures sont en voie de révolutionner le traitement de nos données et d'en accroître la puissance et la valeur : l'avènement de l'ordinateur quantique et l'intelligence artificielle. Ces technologies en plein développement et dont on commence tout juste à entrevoir les implications soulèvent plus que jamais des questions politiques, éthiques et philosophiques majeures.

## **Le besoin d'une recherche et de formations transdisciplinaires**

Ces évolutions rapides et sans précédent induisent des dynamiques intrinsèquement nouvelles par leur nature. Ainsi plus que dans tout autre domaine, la grande intrication d'enjeux d'ordres différents sur les questions numériques nécessite une approche globale. Si les États sont traditionnellement les acteurs de la mise en œuvre d'une vision globale, ils peinent ici à en saisir toutes les dimensions et à passer d'une structure très hiérarchisée et rigide à une structure plus souple et agile. Ils sont alors concurrencés par des acteurs privés, qui, compte tenu de leur caractère global, ont intérêt à dépasser les considérations partisans et géopolitiques étatiques. La question plus spécifique

des enjeux de souveraineté posés par le numérique nécessite donc une vision multidimensionnelle, montrant l'intrication de ces différents enjeux, et analysant leur périmètre, la façon dont ils s'influencent mutuellement et les rapports de forces et rivalités qui en découlent.

Les technologies numériques et leurs conséquences sur nos sociétés modernes invitent donc plus que jamais à jeter des ponts entre les sciences de l'informatique et de l'ingénieur et les sciences humaines et sociales (SHS). Dans un domaine encore très marqué par la dimension technique et industrielle, le rôle des SHS, bien que croissant, en est encore à ces prémises. Pourtant les besoins de penser une approche globale des enjeux de souveraineté est une question urgente pour tenter d'ores et déjà de limiter les effets des dynamiques en cours défavorables à l'Union Européenne et ses États membres.

Aujourd'hui, la construction d'une autonomie stratégique dans le domaine du numérique en France et en Europe demande de relever plusieurs défis analytiques. Il faut d'abord comprendre les dynamiques et les rivalités de pouvoir géopolitiques associées à la révolution numérique notamment par l'exploitation de données en sources ouvertes. Il faut également identifier les enjeux stratégiques à long terme de la transformation numérique, et la façon dont la société civile, les entreprises et les États vont être impactés, saisir les opportunités offertes (économiques, organisationnelles, politiques et stratégique) tout en limitant les menaces croissantes (cyberattaques, cybercriminalités, actions informationnelles etc.

Sélectionné dans le cadre du label « Centre d'Excellence » du Ministère des Armées, le centre de recherche de recherche et de formation GEODE (Géopolitique de la datasphère) vise précisément à étudier les enjeux stratégiques de la révolution numérique et à contribuer à la réflexion stratégique française sur ces sujets. Adossées à la recherche, les formations ont ainsi pour but de diffuser ces

compétences d'analyse stratégique au sein des institutions et des entreprises. Cette tâche est plus particulièrement l'objet du Diplôme de Formation Supérieure Spécialisée d'Université « Révolution numérique : enjeux stratégiques et géopolitiques » (DFSSU, niveau bac+5) dont l'ouverture est prévue en février 2022. Cette formation qui s'adresse spécifiquement aux professionnels (cadres d'entreprises, défense, diplomatie, entre autres) a trait à tous les grands enjeux stratégiques de la révolution numérique pour nos sociétés, et propose également une initiation aux outils permettant d'exploiter les données disponibles en sources ouvertes à des fins d'analyse stratégique (cartographie d'influence informationnelle, réseaux d'acteurs etc.). Autant d'éléments qui doivent de nos jours être pris en compte dans la gestion quotidienne des organisations.

De fait, dans un environnement numérique où les technologies et les réseaux sont partagés entre le monde civil, économique et militaire, les interconnexions, les interactions et les interdépendances sont multiples mais pas toujours bien comprises et maîtrisées. Comprendre les impacts stratégiques de la révolution numérique est donc essentiel pour l'ensemble des acteurs, privés comme publics, d'anticiper les menaces, de prioriser leurs actions et d'identifier les opportunités à saisir. Seule cette réflexion globale permettra d'avancer vers une véritable autonomie stratégique dans le numérique au niveau national comme européen.

<sup>1</sup> Lettre du 1 mars 2021 signée par la chancelière allemande (Angela Merkel) et les Premières ministres du Danemark (Mette Frederiksen), de l'Estonie (Kaja Kallas), et de la Finlande (Sanna Marin) adressée à Ursula von der Leyen, Présidente de la Commission Européenne. Disponible à : <https://valitsus.ee/en/media/3840/download>

<sup>2</sup> Bômont et Cattaruzza, 2020, « Le cloud computing : de l'objet technique à l'enjeu géopolitique. Le cas de la France », Hérodote, n°177-178, La Découverte