LA SOUVERAINETÉ TECHNOLOGIQUE EUROPÉENNE

JANVIER 2022

RENAISSANCE numerique

TABLE DES MATIÈRES

CE QU'IL FAUT RETENIR 4

INTRODUCTION - EN QUÊTE D'UNE DÉFINITION PARTAGÉE 8

Un concept de plus en plus présent dans la politique européenne 9

Un outil discursif qui pâtit d'un manque de définition 11

« Numérique » et « européenne » : des termes qui posent un double enjeu de définition 12

Souveraineté numérique et politique du numérique : des objets souvent confondus 13

PARTIE 1 - UNE NOUVELLE DIMENSION STRATÉGIQUE 14

De la pertinence de l'emploi du terme de « souveraineté » 15

Souveraineté dans le numérique ou impact du numérique sur la souveraineté ? 16

Le numérique comme dimension stratégique 19

PARTIE 2 - DE LA SOUVERAINETÉ NUMÉRIQUE À LA SOUVERAINETÉ TECHNOLOGIQUE 22

La maîtrise de la dimension stratégique numérique repose sur la maîtrise des couches technologiques du numérique 23

La *deep tech* n'est pas le seul levier de souveraineté technologique 24

PARTIE 3 - UNE SOUVERAINETÉ TECHNOLOGIQUE EUROPÉENNE EST-ELLE POSSIBLE ? 28

Un terme absent des traités constitutifs de l'Union européenne 29

Des divergences entre États membres 30

La souveraineté technologique interroge le « pouvoir de pouvoir » de l'Union européenne 31

Une souveraineté technologique qui ne peut être qu'européenne ? 35

CONCLUSION - L'UE DOIT PENSER LE COUPLE « PUBLIC/PRIVÉ » DE MANIÈRE STRATÉGIQUE 36

CE QU'IL FAUT RETENIR

LA QUESTION POSÉE EST CELLE DE LA DÉPENDANCE STRATÉGIQUE DE L'UNION EUROPÉENNE EN MATIÈRE DE NUMÉRIQUE

- Avec la transformation numérique de l'économie et de la société, la quête de souveraineté numérique dépasse le seul périmètre du cyberespace. La transformation numérique interroge l'autonomie des moyens de production et d'action des États et leur capacité à faire respecter leurs intérêts stratégiques.
- Au-delà des tensions inhérentes à la construction européenne, la souveraineté européenne est confrontée à plusieurs sources de menaces induites par le numérique : pressions des États étrangers, pouvoir infrastructurel des « super-plateformes » numériques.
- La crise du Covid-19 a mis sur le devant de la scène la nécessité de ne pas dépendre d'un « robinet technologique » extra-européen pour les technologies stratégiques, c'est-à-dire de ne pas prendre le risque de se voir du jour au lendemain couper l'accès à des technologies essentielles pour l'économie et la société européennes.

LE CONCEPT DE « SOUVERAINETÉ » DOIT ÊTRE CONSIDÉRÉ DANS SON SENS PREMIER AFIN D'ÉTABLIR UN OBJECTIF CLAIR POUR L'UNION EUROPÉENNE

- La souveraineté est une notion historiquement reliée à l'État et son pouvoir d'agir sur un territoire donné : le « pouvoir de pouvoir ».
- L'autonomie stratégique est à la fois un moyen et un dividende de la souveraineté.
- La souveraineté numérique ne vient pas nier la souveraineté classique dans sa conception très physique du territoire d'un État : l'approche territoriale de la souveraineté numérique est particulièrement présente dans les stratégies de certaines puissances, qu'il s'agisse de pays autoritaires confrontés dans leur stratégie géopolitique plus globale à des questions de souveraineté territoriale (par exemple la Chine et la Russie) ou de l'expression par des États de leur puissance au travers d'une présence extraterritoriale (par exemple le *CLOUD Act* américain).

LE NUMÉRIQUE EST UNE NOUVELLE DIMENSION STRATÉGIQUE

- Le numérique doit être pensé comme une nouvelle dimension stratégique, ouverte par les évolutions technologiques et par laquelle transitent et se matérialisent les expressions de la souveraineté des États. Il s'ajoute ainsi au terrestre, au maritime, à l'aérien et au spatial.
- Toutefois, le numérique n'est pas une dimension stratégique comme les autres, car il traverse toutes les autres dimensions. Sa maîtrise permet aux États de confirmer leur souveraineté dans les autres dimensions stratégiques.

RENAISSANCE NUMÉRIQUE INVITE À TRAITER DE LA « SOUVERAINETÉ TECHNOLOGIQUE »

- Sans maîtrise technologique, il n'y a pas d'autonomie stratégique numérique. La maîtrise de la dimension stratégique numérique ne relève pas que du numérique, mais embrasse plus largement un certain nombre de technologies à l'instar des semi-conducteurs.
- Certaines couches technologiques du numérique constituent des prérequis à la garantie de la souveraineté, et il existe pour chacune d'entre elles un seuil critique en dessous duquel la souveraineté technologique n'est pas assurée.
- Allant des matières premières nécessaires à la fabrication des puces électroniques, jusqu'à l'exploitation des données d'usages des services numériques, ces couches incluent une diversité de strates matérielles et de services numériques.
- La politique visant à garantir la souveraineté technologique est une politique de mise en capacité dans un champ d'interdépendances, y compris pour refuser ou réduire sciemment certaines interdépendances au nom d'un objectif de souveraineté. Il s'agit donc pour l'Union européenne d'affirmer sa souveraineté sans se fermer.
- Pour bâtir des politiques industrielles en faveur de sa souveraineté technologique, trois scénarios s'offrent à l'Union européenne : la compétition, la coopétition ou la coopération.

POUR DES RAISONS DE CAPACITÉ D'INVESTISSEMENT, IL N'Y AURA DE SOUVERAINETÉ TECHNOLOGIQUE QU'À L'ÉCHELLE COMMUNAUTAIRE

- Historiquement, l'objectif de souveraineté technologique a appelé des investissements massifs pour maîtriser des chaînes technologiques entières (cf. l'armement, le nucléaire, le spatial).
- L'Union européenne doit ici être considérée comme un levier de puissance pour les États membres.
- Dès lors, en matière de politique de souveraineté technologique, il convient de faire prévaloir le principe de subsidiarité inscrit dans le droit de l'Union européenne.

L'UE DOIT PENSER LE COUPLE « PUBLIC/PRIVÉ » DE MANIÈRE STRATÉGIQUE

- La capacité d'une puissance locale ou régionale à exporter ses technologies est un moyen d'assurer non seulement sa souveraineté technologique, mais également un levier de puissance à l'égard de ses interlocuteurs internationaux.
- L'Union européenne, tout comme la plupart de ses États membres, ne parvient pas encore à s'affranchir d'une conception administrative et judiciaire du rôle de la puissance publique, mêlant une théorisation rigide de ce qu'il incombe à « l'État » de faire ou de ne pas faire et un réflexe de relative méfiance à l'égard des acteurs privés.
- Cette défiance relative à l'égard de la puissance économique freine encore l'avènement d'une méthode partenariale de la puissance européenne, qui devrait nécessairement mêler des intérêts et des acteurs publics et privés.
- L'UE doit désormais – comme le reste du monde – concevoir ses compétences économiques, judiciaires et administratives dans une dimension stratégique et articuler l'indépendance de ses régulateurs sectoriels et transverses avec l'affirmation de ses objectifs stratégiques.

INTRODUCTION

EN QUÊTE D'UNE DÉFINITION PARTAGÉE

UN CONCEPT DE PLUS EN PLUS PRÉSENT DANS LA POLITIQUE EUROPÉENNE

Le concept de « souveraineté numérique », autrefois usité par une poignée d'acteurs, est désormais entré dans la rhétorique au plus haut niveau de la politique européenne. Les récentes déclarations de la Commission et du Conseil européen témoignent de cette volonté grandissante de lui donner un caractère tangible. Dans son discours sur l'état de l'Union en septembre 2020, la présidente de la Commission européenne, Ursula von der Leyen a positionné la souveraineté numérique comme un enjeu pour l'Union européenne (UE)[1]. Les ambitions numériques pour la décennie (*Digital Compass for 2030*) présentées en mars 2021 par la Commission européenne participent de cet objectif[2]. Les conclusions du Conseil européen des 1er et 2 octobre 2020 s'inscrivent également dans cette évolution[3].

La prise de conscience de cet enjeu par les États membres et les institutions européennes a été l'objet d'un processus lent. Deux faits y ont en particulier participé : les révélations d'Edward Snowden et la récente crise sanitaire. En 2013, le lanceur d'alerte Edward Snowden a révélé l'ampleur de la surveillance des agences de renseignement américaines sur les États et institutions étrangers, dont le Conseil européen. Au regard des moyens employés (espionnage d'équipements informatiques, de câbles sous-marins…), cette affaire a mis en lumière la position dominante des États-Unis dans le secteur des infrastructures technologiques[4], en particulier les systèmes d'exploitation et les plateformes de services de masse. Elle a révélé que les États-Unis ont la capacité de collecter des données sensibles dans de nombreux États.

1 Commission européenne, « Discours sur l'état de l'Union de la présidente von der Leyen en session plénière du Parlement européen », 16 septembre 2020 : https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_20_1655

La présidente de la Commission a réitéré ce propos dans son discours sur l'état de l'Union en septembre 2021, évoquant l'enjeu de *« souveraineté technologique européenne »* et invitant à lui accorder *« toute notre attention »*. Commission européenne, « Discours sur l'état de l'Union 2021 de la présidente von der Leyen », 15 septembre 2021 : https://ec.europa.eu/commission/presscorner/detail/fr/SPEECH_21_4701

2 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une boussole numérique pour 2030 : l'Europe balise la décennie numérique », 9 mars 2021 : https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0005.02/DOC_1&format=PDF

3 Dans ces conclusions, les États membres mentionnent l'objectif d'*« assurer notre souveraineté technologique »*, ou encore l'enjeu pour l'Union européenne d'*« être souveraine sur le plan numérique »*. Conseil européen, « Conclusions du Conseil européen, 1er et 2 octobre 2020 » : https://www.consilium.europa.eu/fr/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

4 Pour en savoir plus, voir l'article dédié sur Wikipédia : https://fr.wikipedia.org/wiki/Révélations_d%27Edward_Snowden

L'autre évènement marquant est la crise du Covid-19 qui a débuté en 2020. Cette crise a mis en exergue la forte dépendance des États membres vis-à-vis d'autres États sur des produits essentiels, en particulier dans le domaine de la santé. Cette dépendance stratégique a été aussi un révélateur pour d'autres industries. Pendant la crise, le numérique a permis une certaine résilience de l'économie et de la société. Les services et outils numériques ont été mis à l'épreuve. Ceux qui ont démontré leur fiabilité face à une telle montée en charge ont renforcé de manière significative leur emprise. La crise a révélé leur caractère essentiel et la dépendance dont les Européens faisaient preuve à leur égard. Elle a mis sur le devant de la scène la nécessité de ne pas dépendre d'un « robinet technologique » extra-européen pour les technologies critiques, c'est-à-dire de ne pas prendre le risque de se voir du jour au lendemain couper l'accès à des technologies essentielles pour l'économie et la société européennes. Il est intéressant de noter à ce titre que la Chine privilégie le terme d'autosuffisance à celui d'autonomie, traduisant sa volonté de ne plus être liée aux services et produits étrangers.

> *Avec la crise du Covid, la notion de pénurie est apparue dans le débat politique, et c'est là où le besoin de souveraineté, en termes d'accès à des produits et à des technologies, est devenu plus fort dans les perceptions collectives. [...] Le risque de pénurie significative de biens numériques est devenu tangible, et avec lui le risque d'affecter la stabilité globale de l'économie et de la société, car le numérique touche à tout.*
>
> Thibaut Kleiner,
>
> Directeur « Stratégie et diffusion des politiques », DG CNECT, Commission européenne[5]

5 Audition conduite en janvier 2021 dans le cadre du groupe de travail de Renaissance Numérique sur la souveraineté numérique européenne.

> *Pour nous, au sein du gouvernement allemand, la discussion a toujours porté sur les capacités à mettre en œuvre notre propre politique, sur nos capacités à agir. Nous avons vu, au cours des deux dernières années, que la disponibilité, l'intégrité et le déploiement d'un certain nombre de technologies clés définissent progressivement la capacité d'action des États.*
>
> Nico Geide,
>
> *Policy planner for digital issues*, Ministère fédéral allemand des Affaires étrangères[6]

Ainsi, la transformation numérique rebat les cartes de la souveraineté. Elle interroge l'autonomie des moyens de production et d'action de l'Union européenne et sa capacité à faire respecter ses intérêts stratégiques dans le cas de tensions géopolitiques. Par cela, elle conduit les États européens à revoir la notion même d'alliés[7].

UN OUTIL DISCURSIF QUI PÂTIT D'UN MANQUE DE DÉFINITION

Le concept de « souveraineté numérique » peine pourtant à sortir de sa dimension discursive. De plus en plus présent dans le débat public, il reste vague et englobe une pluralité de perceptions propres aux acteurs qui décident de l'utiliser. D'origine juridique, il devient un concept politique pratique puisque suffisamment large pour que chaque acteur y introduise le sens qu'il souhaite.

6 Citation traduite de l'anglais. Audition conduite en mars 2021 dans le cadre du groupe de travail de Renaissance Numérique sur la souveraineté numérique européenne.

7 Cette observation est notamment portée par les chercheurs Alix Desforges et Didier Danet : *« face à un cyberespionnage qui ne connaît pas la crise, y compris entre alliés, et à la manipulation des données personnelles et des informations sur les grandes plateformes, les États européens ont pris conscience qu'ils ne pouvaient pas se fier aux technologies et services numériques étrangers »*. Danet, D., Desforges, A., « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », Hérodote, 2020/2-3 (N° 177-178), p. 179-195. DOI : 10.3917/her.177.0179. URL : https://www.cairn.info/revue-herodote-2020-2-page-179.htm

Alors que le contexte géopolitique témoigne de la nécessité de se saisir de cet enjeu, il convient d'entamer un travail rigoureux de définition. C'est ce à quoi Renaissance Numérique s'essaie dans cette note. Le groupe de travail du think tank dédié à la « souveraineté numérique européenne » a établi un premier état de l'art de la littérature académique et institutionnelle ayant trait au concept de « souveraineté numérique ». Il en ressort que peu d'acteurs entament un travail préalable rigoureux de définition des termes, centrant la réflexion autour de voies d'action avant d'en fixer les objectifs. Les visions développées par les différents acteurs ne sont en accord ni sur leur étendue, ni sur leurs implications, ni même sur les termes. Cette notion est aussi parfois en concurrence avec d'autres comme celle d'« autonomie stratégique », malgré leur imbrication.[8] Une enquête publiée en mars 2021 par les fondations Jean Jaurès et Friedrich Ebert illustre, à ce titre, le flou qui existe autour des notions de « souveraineté » et de « souveraineté européenne » et la grande diversité des perceptions entre les États membres.[9]

« NUMÉRIQUE » ET « EUROPÉENNE » : DES TERMES QUI POSENT UN DOUBLE ENJEU DE DÉFINITION

Si les discours actuels peinent à donner un sens clair à la notion de « souveraineté », qui fait pourtant l'objet d'une définition juridique bien établie[10], l'exercice est rendu encore plus difficile quand il s'agit de définir le concept de « souveraineté numérique européenne ». Les deux qualificatifs associés au terme de souveraineté revêtent eux-mêmes des enjeux de définition. Concernant l'emploi du terme « numérique », il convient de s'interroger sur ce qui est visé et ainsi ce qu'il désigne : le cyberespace ou les différentes couches technologiques du numérique ? Par ailleurs, associé à la souveraineté, le terme peut avoir deux sens. S'agit-il d'évoquer la souveraineté dans le numérique ou l'impact du numérique sur la souveraineté ? Concernant le concept de « souveraineté européenne », ce dernier s'inscrit dans une tension inhérente à la construction européenne, à savoir s'il est possible de l'envisager alors que la souveraineté est une notion directement rattachée à l'État.

SOUVERAINETÉ NUMÉRIQUE ET POLITIQUE DU NUMÉRIQUE : DES OBJETS SOUVENT CONFONDUS

Étant donné que le concept de souveraineté numérique demeure flou, il n'a pas été un objet réel de la politique publique du numérique. Le plus souvent, les acteurs commencent par concevoir la politique du numérique avant de définir l'objectif de souveraineté numérique. Le périmètre large du rapport de la mission parlementaire « Bâtir et promouvoir une souveraineté numérique nationale et européenne »[11] en est une illustration.

La souveraineté numérique et la politique du numérique ne se confondent pas. La politique publique du numérique peut aider à bâtir ou renforcer une souveraineté numérique. La souveraineté numérique offre quant à elle la latitude aux États pour définir leur politique du numérique.

C'est pourquoi il est important de distinguer la politique visant à garantir la souveraineté numérique d'une politique du numérique protectionniste. La politique visant à garantir la souveraineté numérique est une politique de mise en capacité dans un champ d'interdépendances, y compris pour refuser ou réduire sciemment certaines interdépendances au nom d'un objectif de souveraineté. Il s'agit donc pour l'Union européenne d'affirmer sa souveraineté sans se fermer. À ce titre, la Commission européenne a récemment employé le concept d'« autonomie stratégique ouverte »[12]. Derrière ces enjeux, est posée la question du niveau acceptable de dépendance pour l'Europe : en dessous de quel seuil de dépendance numérique l'UE perd-elle la maîtrise de sa souveraineté ?

8 Voir à ce sujet la partie « De la pertinence de l'emploi du terme de « souveraineté » » de la présente note, pp. 15-16.

9 Elle a été réalisée par l'institut Ipsos auprès de 8 000 citoyens européens répartis dans huit pays (France, Allemagne, Italie, Espagne, Pologne, Lettonie, Roumanie, Suède). « De la souveraineté européenne », Fondation Jean Jaurès et Fondation Friedrich Ebert, 1er mars 2021 : https://www.jean-jaures.org/publication/de-la-souverainete-europeenne/

10 Voir sur ce point la première partie de cette note.

11 Assemblée nationale, « N° 4299 tome 1 - Rapport d'information de M. Philippe Latombe fait au nom de la mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » », 29 juin 2021 : https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

12 Commission européenne, "2021 Strategic Foresight Report. The EU's capacity and freedom to act", 8 septembre 2021 : https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2021-strategic-foresight-report_en

PARTIE 1
UNE NOUVELLE DIMENSION STRATÉGIQUE

DE LA PERTINENCE DE L'EMPLOI DU TERME DE « SOUVERAINETÉ »

Dans cet exercice de définition, Renaissance Numérique défend l'emploi du terme de souveraineté dans sa stricte signification. Loin de la connotation négative qui lui est fréquemment attribuée en France, l'associant au nationalisme ou au protectionnisme, le think tank invite à considérer ce concept dans son sens premier afin d'établir un objectif clair pour l'Union européenne.

La souveraineté est une notion historiquement reliée à l'État et son pouvoir d'agir sur un territoire donné : le « pouvoir de pouvoir[13] » . En droit international, elle est définie comme la capacité d'un État à affirmer son existence et sa volonté propre à l'intérieur comme à l'extérieur de son territoire. À l'extérieur, l'état de souveraineté se fonde alors sur un principe de reconnaissance mutuelle[14].

Les débats confondent souvent « souveraineté » et « autonomie stratégique » avec pour chacun des termes leurs porte-flambeaux. Si les concepts de souveraineté et d'autonomie stratégique sont étroitement imbriqués, ils ne se situent pas au même niveau. L'autonomie stratégique est à la fois un moyen et un dividende de la souveraineté. À la différence de l'indépendance, elle permet de considérer l'état de la mondialisation et les contraintes inhérentes aux interdépendances des chaînes de production. Le concept d'autonomie stratégique est directement importé du secteur de la défense, notamment français : *« L'autonomie stratégique est perçue comme le moyen pour un État d'exercer sa souveraineté [RS2017 ; LBDSN 2008, 2013]. Elle vise à détenir une « capacité autonome d'appréciation, de décision et d'action » »*.[15] [16]

13 *« Issue de la philosophie politique où elle se restreint à l'idée de souveraineté nationale, la souveraineté peut se définir comme la capacité pour une entité de se donner ses propres règles ou, plus trivialement, comme « le pouvoir de pouvoir ». »* J.-G. Ganascia, E. Germain, C. Kirchner (2018), « La souveraineté à l'ère du numérique. Rester maîtres de nos choix et de nos valeurs », CERNA : http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf

14 Selon Pierre Avril et Jean Gicquel, la souveraineté *« signifie, négativement, l'absence de toute dépendance extérieure et de tout empêchement intérieur. Positivement, [elle] désigne le caractère suprême de la puissance étatique, et cette puissance elle-même, c'est-à-dire les pouvoirs effectifs compris dans la puissance de l'État. La souveraineté emporte donc à la fois l'indépendance dans l'ordre international (la souveraineté de l'État), le pouvoir exclusif et sans limite, sinon celles que l'État de droit s'assigne à lui-même, dans l'ordre interne (souveraineté dans l'État), et le contenu de ce pouvoir. »* Avril, P., Gicquel, J., *Lexique de droit constitutionnel*, Paris, PUF, 2003.

15 Danet, D., Desforges, A., *op. cit.*

16 Cette approche rejoint d'autres définitions de l'autonomie stratégique. Paul Timmers propose la définition suivante (traduite de l'anglais) : *« L'autonomie stratégique est l'aptitude, en termes de capacités et de moyens, à décider et à agir sur les aspects essentiels de son futur au long terme dans l'économie, la société et les institutions. »* Timmers, P., "Cybersecurity is forcing a rethink of strategic autonomy", OXPOL, 14 septembre 2018 : https://blog.politics.ox.ac.uk/cybersecurity-is-forcing-a-rethink-of-strategic-autonomy/#cybersecurity%20%20#strategic_autonomy%20#sovereignty

Pour qu'un État soit souverain, cette capacité doit être irréductible, d'où la nécessité de penser clairement la souveraineté numérique dès lors que le numérique est devenu une composante *sine qua non* du « pouvoir de pouvoir » et qu'il est quasi-exclusivement privatisé.[17]

> *Beaucoup voient la question de la souveraineté comme une question d'hégémonie. Or, nous la voyons comme une question d'autonomie stratégique.*
>
> Henri Verdier,
> Ambassadeur pour le Numérique de la France[18]

SOUVERAINETÉ DANS LE NUMÉRIQUE OU IMPACT DU NUMÉRIQUE SUR LA SOUVERAINETÉ ?

Le concept de « souveraineté numérique » pourrait revêtir deux sens et traiter à la fois d'un enjeu de souveraineté dans le cyberespace et de l'impact du numérique sur la souveraineté.[19] Toutefois, si on retient la définition stricte de la souveraineté liée à l'État et à son « pouvoir de pouvoir » sur ce qu'il considère être son territoire, c'est la deuxième interprétation qui s'avère pertinente et qui est retenue ici. Avec la transformation numérique de l'économie et de la société, la quête de souveraineté numérique dépasse le seul périmètre du cyberespace.

17 Par extension au champ numérique, Resa Mohabbat Kar et Basanta E. P. Thapa définissent l'autonomie stratégique comme : *« la capacité de l'État à mettre en œuvre ses propres priorités politiques, sociales et économiques, sans être limité à un niveau non voulu par les dépendances de la numérisation ».* Mohabbat Kar, R., Thapa B. E. P., "Digitale Souveränität als Strategische Autonomie", Kompetenzzentrum Öffentliche IT, septembre 2020 : https://www.oeffentliche-it.de/publikationen. Cité dans Christakis, T., "European Digital Sovereignty": Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", 18 décembre 2020 : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098

18 Audition conduite en janvier 2021 dans le cadre du groupe de travail de Renaissance Numérique sur la souveraineté numérique européenne.

19 Sur ce sujet, lire Pierre-Yves Quiviger, « Une approche philosophique du concept émergent de souveraineté numérique », *Nouveaux Cahiers du Conseil Constitutionnel* n° 57 (Dossier : Droit constitutionnel à l'épreuve du numérique), octobre 2017 : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/une-approche-philosophique-du-concept-emergent-de-souverainete-numerique
L'auteur évoque notamment : *« La principale difficulté par rapport à la notion de souveraineté numérique tient à l'ambivalence d'une formule à laquelle la langue française permet d'accorder deux acceptions : la souveraineté sur le numérique, le numérique étant alors ce sur quoi porte la souveraineté, ou le champ dans lequel la souveraineté peut rencontrer une limite ou avoir vocation à se manifester plus fermement (ou non) [...] un autre sens de l'expression « souveraineté numérique » à savoir, en un sens minimaliste, les manifestations numériques de la souveraineté (l'écart est alors mince mais non nul avec la première souveraineté, portant sur le numérique) ».*

Eu égard à son caractère transversal, la transformation numérique affecte l'exercice de la souveraineté dans de multiples dimensions : économie, alimentation[20], santé, culture, éducation, défense, sécurité[21], etc. Elle influe sur la nature même des régimes politiques[22]. Elle effrite la souveraineté au sens le plus classique du terme : l'Union européenne peut-elle encore faire – c'est-à-dire adopter et faire appliquer – les règles qu'elle souhaite ?

Au-delà des tensions inhérentes à la construction européenne[23], la souveraineté européenne est confrontée à plusieurs sources de menaces induites par le numérique. L'Union européenne fait face à des États étrangers à même de conduire des cyberattaques ou du cyberespionnage à l'encontre de ses institutions ou de ses États membres, ou d'user du « robinet technologique » comme levier de pression. Des « super-plateformes »[24] numériques viennent quant à elles empiéter sur les pouvoirs des États. Si leur pouvoir n'est pas absolu, ces entreprises réunissent des composantes inhérentes à la souveraineté. Le chercheur Henri Isaac évoque à ce titre leur « pouvoir infrastructurel »[25]. Elles délimitent des espaces qui participent de l'espace démocratique et étatique et y imposent leurs propres normes et langage. Elles véhiculent une littératie qui leur est propre au travers de leurs services. Elles sont capables de s'adresser à des populations plus profondément que les gouvernements eux-mêmes et, partant, d'influencer le champ politique dans le sens de leurs modèles économiques et sociétaux. Elles développent une collecte massive de données et une capacité d'analyse à des fins qui leur sont propres, peut-être sans équivalent au sein des États pris isolément. Dès lors, elles mettent en difficulté le pouvoir des États car ce ne sont pas des

20 La captation des données agricoles est par exemple devenue un enjeu de souveraineté. Voir Bounaud, P., Pouyat, M., « Données agricoles en Europe : défendre notre valeur commune », Renaissance Numérique, tribune, 21 mai 2019 : https://www.renaissancenumerique.org/publications/donnees-agricoles-en-europe-defendre-notre-valeur-commune

21 À ce titre, Alix Desforges et Didier Danet rappellent que : *« la révolution numérique vient effectivement bouleverser les modalités de l'exercice de cette souveraineté parce qu'elle permet des activités transfrontières et aussi parce qu'elle offre des moyens d'action à distance pour espionner et saboter des réseaux en dissimulant son identité et en s'abritant derrière des juridictions multiples. »* Danet, D., Desforges, A., *op. cit.*

22 Si on tire grossièrement le fil, les régimes libéraux doivent se prémunir contre l'ingérence de bulles informationnelles quand les régimes autoritaires doivent se prémunir contre la libre circulation de l'information.

23 Voir, dans la présente note, la partie « Une souveraineté technologique européenne est-elle possible ? » pp. 28-35.

24 Ce terme est défini par le chercheur Henri Isaac et désigne notamment les acteurs suivants : Google, Facebook, ByteDance, Tencent, Microsoft et Alibaba. H. Isaac, (2021), « L'irrésistible montée en puissance des super-plateformes numériques », *Questions Internationales*, n°109, septembre.

25 Sur ce sujet, Henri Isaac propose une grille d'analyse du pouvoir des « super-plateformes » numériques en se fondant sur la distinction entre le « pouvoir despotique » et le « pouvoir infrastructurel » des États établie par Michael Mann.

capacités faciles à reconstruire. Le renforcement du contrôle de l'État chinois sur ses géants numériques témoigne de cette tension entre les États et ces grands acteurs de la *tech*[26]. Ces différentes sources de menaces peuvent d'ailleurs s'imbriquer. Dans le champ du renseignement, par exemple, le renseignement d'origine publique et le renseignement d'origine privée s'intriquent mécaniquement. Enfin, ces entreprises sont non européennes et ont parfois elles-mêmes un lien d'allégeance avec leur État d'origine et soumis à des législations extraterritoriales.

Si la souveraineté numérique ne se résume pas au cyberespace, elle ne vient pas nier la souveraineté classique dans sa conception très physique du territoire d'un État[27]. L'approche territoriale de la souveraineté numérique est particulièrement présente dans les stratégies de certaines puissances, qu'il s'agisse de pays autoritaires confrontés dans leur stratégie géopolitique plus globale à des questions de souveraineté territoriale (par exemple la Chine et la Russie) ou de l'expression par des États de leur puissance au travers d'une présence extraterritoriale. À ce titre, le *CLOUD Act* américain est une projection extraterritoriale de la souveraineté qui consiste à présumer, lorsque des services ont été exportés par des acteurs technologiques ou économiques considérés comme rattachés à un État souverain d'origine, que l'accès par cet État s'étend à toutes les données traitées par ces acteurs où qu'elles et qu'ils soient dans le monde et donc, que l'application territoriale de la loi n'a pas d'autre frontière que le lien capitalistique, y compris indirect[28], pour permettre leur récupération par les autorités de cet État.

26 « De Jack Ma à TikTok, pourquoi Pékin reprend le contrôle des géants de la tech chinoise », Bogdan Bodnar, *Business Insider France*, 26 mai 2021 : https://www.businessinsider.fr/de-jack-ma-a-tiktok-pourquoi-pekin-reprend-le-controle-des-geants-de-la-tech-chinoise-187637

27 Le député Philippe Latombe et les membres de sa mission parlementaire l'ont bien exprimé dans leur rapport : *« le numérique ne vient pas remettre fondamentalement en cause la souveraineté des États, il rebat simplement les cartes des relations de pouvoir entre ces derniers au niveau international et constitue un puissant levier d'influence à court et moyen terme »*. Assemblée nationale, *op. cit.*

28 Les entreprises soumises au *CLOUD Act* sont les entreprises détenues directement ou indirectement par un acteur américain.

LE NUMÉRIQUE COMME DIMENSION STRATÉGIQUE

Le numérique doit ainsi être pensé comme une nouvelle dimension stratégique, ouverte par les évolutions technologiques. Il s'agit d'interroger la stratégie de l'Union européenne en observant si et comment elle entend se doter de moyens numériques critiques et de leviers d'action sur ces moyens, nécessaires à la garantie de sa souveraineté. Le numérique constitue une cinquième dimension stratégique s'ajoutant au terrestre, au maritime, à l'aérien et au spatial, par laquelle transitent et se matérialisent les expressions de la souveraineté des États. Dès lors, il s'agit d'identifier les spécificités de cette nouvelle dimension.

L'émergence des domaines aérien et spatial dans la stratégie des États (grâce aux avancées technologiques qui en ont fait des terrains de puissance) constitue un exemple pertinent pour saisir les enjeux liant la souveraineté au numérique. L'espace aérien et l'espace spatial questionnent les représentations du territoire. S'agrégeant aux autres dimensions stratégiques déjà maîtrisées (mer, terre), elles occupent une fonction spécifique. Aussi bien dans l'espace aérien que dans l'espace spatial, le théoricien Hervé Coutau-Bégarie souligne un double phénomène central qui vient redéfinir les rapports de force entre les acteurs du jeu stratégique : *« la dilatation de l'espace et la contraction du temps »*. L'espace aérien a permis *« l'unification des espaces stratégiques »*, en créant de nouveaux mécanismes d'intermédiation avec une réduction du temps nécessaire à connecter les acteurs du jeu stratégique. Avec l'espace, ce double phénomène se matérialise, par exemple, à travers la transformation provoquée par les satellites. C'est grâce à ces nouvelles technologies, selon l'auteur, que la Terre est devenue pour la première fois un *« théâtre véritablement unifié, qu'un commandement centralisé peut contrôler en temps réel et en continu »*. Selon Hervé Coutau-Bégarie, l'espace spatial intervient dans *« toutes les composantes de la stratégie »*, mais également d'une manière différente. En effet, la *« prédominance des systèmes passifs sur les systèmes actifs (ou agressifs) »* par rapport aux autres dimensions stratégiques est la caractéristique principale du spatial : *« Alors que les fonctions des systèmes terrestres, maritimes ou aériens sont d'abord tournés vers le combat, les systèmes spatiaux sont orientés vers le tryptique*

29 Coutau-Bégarie, H. (2011), *Traité de stratégie*, Economica, 7e édition.

Voir-Écouter-Communiquer, c'est-à-dire vers des fonctions d'observation et de communication au service des autres milieux »[29]. Les États ont ainsi longtemps exclu le déploiement d'armes dans l'espace et utilisent majoritairement cette dimension pour implanter des dispositifs de surveillance. En cela, l'espace joue encore un rôle de stabilisateur de l'ordre international. La dimension stratégique numérique se distingue également de l'espace en ce que les moyens numériques font l'objet et participent à de nombreuses attaques. En cela, elle ne peut être considérée comme un élément actif au service de la stabilité de l'ordre international. Il s'agit d'une dimension travaillée de l'intérieur par une logique d'affrontement.

Le numérique, nouveau facteur de puissance, de type mouvant, n'est pas une dimension stratégique comme les autres. Il est difficile de le comparer avec les dimensions stratégiques précédentes, car cela implique partiellement de concevoir le numérique comme un domaine à part alors qu'il traverse tous les autres. La maîtrise de cette dimension permet de confirmer sa souveraineté dans les autres dimensions stratégiques. Elle influe aussi sur les relations existantes entre les différentes dimensions stratégiques. Ceci est rendu possible par le développement de nouveaux modes d'intermédiation. Grégoire Germain et Paul Massart illustrent ce rôle spécifique au travers de l'exemple des infrastructures numériques qui *« se développent aussi bien à terre (serveurs), en mer (câbles sous-marins), dans l'air et dans l'espace exo-atmosphérique pour certains segments spatiaux, notamment en matière de système de combat militaire »*.[30] Par ailleurs, le numérique est une dimension stratégique qui se caractérise par une capacité à se dilater à la différence des autres dimensions.

30 Germain, G., Massart, P., « Souveraineté numérique », Études, 2017/10 (Octobre), p. 45-58. DOI : 10.3917/etu.4242.0045. URL : https://www.cairn.info/revue-etudes-2017-10-page-45.htm

PARTIE 2
DE LA SOUVERAINETÉ NUMÉRIQUE À LA SOUVERAINETÉ TECHNOLOGIQUE

LA MAÎTRISE DE LA DIMENSION STRATÉGIQUE NUMÉRIQUE REPOSE SUR LA MAÎTRISE DES COUCHES TECHNOLOGIQUES DU NUMÉRIQUE

Définir un objectif clair pour l'Union européenne nécessite d'être précis sur les termes employés. Pour investir une nouvelle dimension stratégique (ici le numérique), il ne faut pas être dépendant de l'extérieur. Or, la maîtrise de la dimension stratégique numérique ne relève pas que du numérique, mais embrasse plus largement un certain nombre de technologies à l'instar des semi-conducteurs[31]. Sans maîtrise technologique, il n'y a pas d'autonomie stratégique numérique. C'est pourquoi Renaissance Numérique invite à traiter de la « souveraineté technologique » plutôt que de la « souveraineté numérique ».

> *Certaines des technologies pertinentes ici ne sont pas numériques, comme l'informatique quantique par exemple. « Numérique » n'est pas le concept que nous utilisons. Nous utilisons les termes « souveraineté technologique ». La « souveraineté technologique » est la capacité à développer, déployer, appliquer, sourcer et garantir l'intégrité d'un certain nombre de technologies clés qui sont devenues des instruments de pouvoir en cette période de compétition géopolitique que nous vivons. Les plus pertinentes pourraient être l'IA, le* cloud computing, *les semi-conducteurs et toute la chaîne de valeur qui en découle.*
>
> Nico Geide,
>
> *Policy planner for digital issues*, Ministère fédéral allemand des Affaires étrangères[32]

31 Pour en savoir plus, lire la page dédiée sur Wikipédia : https://fr.wikipedia.org/wiki/Semi-conducteur

32 Audition conduite en mars 2021 dans le cadre du groupe de travail de Renaissance Numérique sur la souveraineté numérique européenne.

Il s'agit pour l'Union européenne de vérifier les conditions de garantie d'un état de souveraineté. Un enjeu de souveraineté se dégage dans un certain nombre de couches technologiques du numérique, allant des matières premières nécessaires à la fabrication des puces, jusqu'à l'exploitation des données d'usages des services numériques. La plupart des acteurs puissants cherchent à avoir un modèle intégré, c'est-à-dire une maîtrise verticale de ces couches. L'UE a des forces dans certaines couches technologiques, mais n'en maîtrise pas l'intégralité qui la rendrait indépendante. Elle ne peut pas disposer, par elle-même, de tous les éléments composant chaque couche, d'autant que les technologies du numérique sont souvent de nature ouverte. Néanmoins, elle peut prendre certaines voies qui lui permettront, à l'avenir, d'atteindre un degré supérieur de maîtrise sur ces différentes strates, que ce soit en renforçant sa capacité à produire ou par d'autres leviers.

LA *DEEP TECH* N'EST PAS LE SEUL LEVIER DE SOUVERAINETÉ TECHNOLOGIQUE

Ce travail d'identification est important et doit permettre d'établir des stratégies pertinentes loin des incantations en faveur de la construction de géants numériques européens. Ceci ne veut pas dire que cet objectif n'a pas sa place dans une stratégie pour garantir la souveraineté technologique européenne. Mais pour le savoir, il convient de déterminer ce qui est nécessaire pour garantir une suffisance stratégique en cas de crise de basse ou de haute intensité. Certaines couches technologiques constituent des prérequis à la garantie de la souveraineté, et il existe pour chacune d'entre elles un seuil critique en dessous duquel la souveraineté technologique n'est pas assurée. Ces strates ne correspondent pas nécessairement à de la *deep tech*, et incluent une diversité de couches matérielles et de services numériques[33]. Il s'agit d'identifier ces couches et seuils critiques de dépendance, de savoir où en est l'UE dans ces différents domaines et de bâtir des politiques industrielles pour les atteindre.

33 Renaissance Numérique mène actuellement une recension des couches technologiques du numérique qui revêtent des enjeux de souveraineté pour l'Union européenne. Ce travail, qui est en cours, retrace une diversité de couches telles que les matières premières, les microprocesseurs, les grandes plateformes numériques, les protocoles d'Internet ou encore l'informatique quantique (liste non exhaustive).

Dès lors, trois scénarios s'offrent à l'UE : la compétition, la coopétition ou la coopération. Le premier scénario (compétition) consiste à créer des champions européens du numérique pour concurrencer les grands acteurs existants ou à bâtir les grands concurrents de demain. Ce scénario nécessite des investissements publics et privés conséquents et des écosystèmes organisés pour favoriser l'émergence de tels acteurs. Il s'inscrit donc souvent dans le moyen-long terme.

Le deuxième scénario (coopétition) consiste à bâtir des alliances industrielles entre acteurs privés européens existants. Il s'agit d'identifier les acteurs qui se rapprochent des seuils critiques visés et de réfléchir à leur alliance afin qu'ils puissent prendre des parts de marché. Dans cette optique, l'Union européenne pourrait également encourager des politiques d'investissement pour s'accaparer des briques technologiques qui existent à l'étranger comme ont su le faire des acteurs extra-européens en Europe.

Enfin, le troisième scénario (coopération) consiste à sortir des logiques d'enfermement établies jusqu'à présent par certains grands acteurs de la *tech* et d'obliger à une interopérabilité forte de technologies stratégiques par l'imposition de standards partagés. GAIA-X[34] s'inscrit directement dans ce scénario. Cette initiative est à saluer au sens où elle montre que le besoin d'une démarche commune au niveau européen a été identifié. Toutefois, elle comporte des vulnérabilités liées à un manque de maturité dans son exécution, comme l'illustrent les conditions d'adhésion qui reposent essentiellement sur un critère de territorialité et ne tiennent pas compte de la nationalité des acteurs. Cette voie ne supprime pas complètement le problème de la dépendance puisqu'elle incarne l'état de l'offre européenne au regard de ses compétiteurs mondiaux. Ce projet qui se voulait souverain démontre l'incomplétude actuelle de l'offre européenne – par manque d'intégration entre infrastructures et services – puisqu'il ne permet de créer une chaîne intégrée d'infrastructures et de services qu'en y accueillant des acteurs extra-européens venant combler les trous non satisfaits par une offre européenne morcelée. Cela conduit GAIA-X à manquer sa cible – et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) à envisager en France de durcir ses critères de cer-

34 Pour en savoir plus, voir le site dédié au projet : https://www.gaia-x.eu

tification[35] –, car les acteurs non européens qui y participent sont soumis à l'extra-territorialité des lois et sont en porte-à-faux avec l'arrêt Schrems II de la Cour de Justice de l'Union européenne (CJUE)[36], ce qui fait perdre l'objectif initial d'un « coffre » européen exempt de toute influence extra-européenne.

L'approche française mise en œuvre par l'ANSSI avait reposé jusqu'à présent sur la possibilité de bâtir des offres exemptes de toute influence légale extra-communautaire sans s'interdire de faire appel à des acteurs extra-européens. L'agence doit désormais s'adapter à la décision « Schrems II », qui prescrit aux États membres, aux administrations, comme aux entreprises européennes, de s'affranchir des effets en Europe, des lois des pays non européens.

Lorsque ces lois extra-territoriales sont portées par la nationalité de l'actionnaire principal d'une filiale européenne fournissant des prestations informatiques, il ne suffit plus d'établir en Europe des filiales, ni d'y héberger des données dans des *data centers* européens, ni même d'y conclure des contrats informatiques régis exclusivement par le droit local européen, ni même de promettre aux autorités européennes qu'on violera, à la première demande, les injonctions de soumission aux lois extra-territoriales auxquelles la nationalité de la société-mère soumet sa filiale européenne.

Le lien capitalistique de rattachement à une « mère » non européenne – américaine, par exemple – est désormais présumé problématique par le droit européen. Même si ce problème qui surgit d'une décision de la CJUE ne trouve pas de solution pratique immédiate, il implique nécessairement de concevoir les chaînes de prestations informatiques à l'aune de la nationalité des entreprises et de celle de leurs actionnaires et non plus seulement, en fonction de la territorialité du service informatique fourni ou de l'établissement d'une filiale et de ses infrastructures informatiques.

35 Voir à ce titre la révision du référentiel « SecNumCloud ». Agence nationale de la sécurité des systèmes d'information, « Prestataires de services d'informatique en nuage (SecNumCloud). Référentiel d'exigences », Partie « 19.6 Immunité au droit extracommunautaire », Version 3.2.a du 21 septembre 2021 : https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a_revision.pdf

36 Renaissance Numérique (2021), « Arrêt Schrems II : Comment sortir de l'impasse ? » : https://www.renaissancenumerique.org/publications/arret-schrems-ii-comment-sortir-de-l-impasse

PARTIE 3
UNE SOUVERAINETÉ TECHNOLOGIQUE EUROPÉENNE EST-ELLE POSSIBLE ?

Telle que la souveraineté a été définie, il est possible de s'interroger sur la pertinence de viser une souveraineté technologique européenne. Le concept de souveraineté se rattache à une dimension nationale dans sa définition classique. Comment peut-on dès lors l'envisager à un niveau supranational, ici européen, face à d'autres entités plus unifiées, qu'elles soient centralisées (Chine) ou fédérales (États-Unis) ? Cette interrogation rejoint une problématique classique de la souveraineté technologique (cf. l'armement, le nucléaire, le spatial), à savoir que, historiquement, l'objectif de souveraineté technologique a appelé des investissements massifs pour maîtriser des chaînes technologiques entières. Le marché des semi-conducteurs est à ce titre significatif. Il s'agit d'une industrie de concentration importante à capital massif, nécessitant des dizaines d'années d'investissements afin de réaliser les produits de dernière génération. Dans les prochains mois, les États-Unis devraient par exemple allouer 52 milliards de dollars de financement pour subventionner la construction d'usines de pointe aux États-Unis[37]. De même, le montant total des dépenses en Recherche et Développement des « super-plateformes » numériques (hors ByteDance) équivaut à un peu plus de sept fois le budget européen de la recherche pour l'année 2020 (97,4 milliards de dollars contre 11 milliards d'euros)[38]. De tels montants ne peuvent exister qu'à l'échelle européenne.

UN TERME ABSENT DES TRAITÉS CONSTITUTIFS DE L'UNION EUROPÉENNE

Les questionnements sur la nature européenne de la souveraineté technologique rejoignent les interrogations liées à la construction et à l'intégration européennes.[39] L'Union européenne est une entité politique qui fonde sa construction sur un principe de délégation de souveraineté et non de souveraineté. Le terme de souveraineté n'apparaît d'ailleurs nulle part dans les

37 Eurasia Group, "EU/Geo-technology: Semiconductor push will cost billions, take years, and still not deliver self-sufficiency", 4 novembre 2021.

38 H. Isaac, (2021), *op. cit.*

39 Pierre Avril et Jean Gicquel rappellent à ce titre que d'un point de vue constitutionnel, la souveraineté est *« l'apanage de l'État, à l'opposé d'une organisation internationale (Union européenne) qui ne peut bénéficier que de transferts de compétences consentis par les États membres. »* Avril, P., Gicquel, J. (2003), *op. cit.*

traités constitutifs de l'Union européenne[40] [41] à la différence de textes constitutionnels nationaux qui évoquent la « souveraineté nationale » comme la Constitution française[42]. L'état actuel du débat sur la forme juridique que doit prendre l'Union européenne n'est pas propice à la consécration juridique d'une souveraineté européenne. Toutefois, elle est déjà un enjeu géopolitique et démocratique tangible faisant écho aux enjeux de souveraineté de ses États membres.

DES DIVERGENCES ENTRE ÉTATS MEMBRES

Mais est-il possible d'atteindre une souveraineté technologique au niveau européen au vu de ces enjeux d'intégration et du prérequis qu'est la volonté politique commune des États membres de s'engager dans cette voie ? Actuellement, il n'existe pas de vision partagée sur l'emploi du concept de « souveraineté technologique européenne » et sur ce qu'il englobe.

Tous les États membres n'ont pas officiellement pris position sur le développement d'une souveraineté technologique européenne et ceux qui s'accordent sur cette nécessité ne le font pas avec les mêmes termes et/ou le même niveau d'ambition[43]. Selon la maturité de leur économie numérique, leur histoire socio-culturelle, les États membres n'y ont pas le même intérêt[44]. Le lien qui relie les États d'Europe de l'Est aux États-Unis pour se défendre vis-à-vis de la Russie participe, par exemple, de la distanciation de ces pays vis-à-vis de ce concept d'autonomie européenne. De même, le niveau des économies numériques française et allemande par rapport à des États européens plus petits nourrit l'attention portée à cet enjeu dans ces pays.

40 Christakis, T., *op. cit.*

41 Les traités constitutifs de l'Union européenne sont recensés sur le site du droit de l'Union européenne, EUR-Lex : https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-founding.html?locale=fr

42 Conseil constitutionnel, « Texte intégral de la Constitution du 4 octobre 1958 en vigueur », Texte intégral en vigueur à jour de la révision constitutionnelle du 23 juillet 2008 : https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur

43 Alix Desforges et Didier Danet citent à ce titre une étude du think tank European Council of Foreign Relations de 2019 qui *« montre que les États membres ne soutiennent pas tous le développement d'une autonomie stratégique européenne et que ceux qui le font ne s'accordent ni sur ce qu'elle recouvre, ni « sur le niveau d'ambition géographique et fonctionnel qu'ils devraient adopter » pour la mettre en œuvre ».* Danet, D., Desforges, A., *op. cit.*

44 Assemblée nationale, *op. cit.*

LA SOUVERAINETÉ TECHNOLOGIQUE INTERROGE LE « POUVOIR DE POUVOIR » DE L'UNION EUROPÉENNE

Poser la question de la souveraineté technologique conduit à se questionner sur la réalité du « pouvoir de pouvoir » de l'Union européenne. L'Union européenne peut-elle être puissante sans les attributs traditionnels de la souveraineté ? À certains égards, l'UE possède déjà des ingrédients de puissance en matière de numérique, notamment par le biais de la régulation de l'économie numérique. Ce pouvoir de régulation se traduit par la capacité de l'Union à sanctionner la violation de ses propres règles par des acteurs extra-européens et aussi à sanctionner localement les violations de ses propres règles par des États membres. Elle s'exprime également par la reconnaissance de ce pouvoir à l'étranger. La professeure Anu Bradford a théorisé cette reconnaissance au travers du concept de « l'Effet de Bruxelles » (le *Brussels effect*)[45] qui illustre la capacité de l'UE à inspirer des régulations étrangères. Un des exemples les plus fréquemment cités est celui du Règlement général sur la protection des données (RGPD). Toutefois, si ce dernier témoigne de la capacité de l'UE à bâtir une projection extraterritoriale de son droit, ce règlement n'a pas été pensé comme un instrument de puissance, mais plutôt comme un outil de protection des citoyens européens. Le RGPD illustre également que ce type de « puissance juridique » peut s'avérer relativement limité quand *"code is law"*, selon la célèbre formule de Lawrence Lessig[46]. L'application du règlement par Google – avec le *Privacy Sandbox*[47] – et Apple – avec l'*App Tracking Transparency*[48] – est à ce titre illustrative, alors que ces acteurs imposent, par leur infrastructure, leurs propres normes à leur écosystème pour se mettre en adéquation avec le cadre européen.

Par ailleurs, l'application de ce droit reste défensive et ne s'affirme qu'*a posteriori*, de façon marginale. Elle dépend de sa judiciarisation et de l'interprétation indépendante d'un juge. Avec l'arrêt Schrems II, la Cour de Justice de l'Union européenne a, par exemple, provoqué une direction politique qu'aucun État

45 Christakis, T., *op. cit.*

46 Lessig, L. (2000), "Code is law, On Liberty in Cyberspace", *Harvard magazine* : https://www.harvardmagazine.com/2000/01/code-is-law-html

47 Pour en savoir plus, voir le site de l'initiative : https://privacysandbox.com

48 Pour en savoir plus, voir le site de l'initiative : https://developer.apple.com/documentation/apptrackingtransparency

membre n'avait donné jusqu'à présent sur la protection des données, en faisant grief à un prestataire informatique d'être soumis à des lois extra-territoriales produisant leurs effets sur ses filiales et prestations informatiques européennes. Cette décision s'applique désormais comme une règle nouvelle, sans qu'aucun législateur européen n'en ait fait le choix politique résolu. Dans le même temps, la même Cour de Justice a invalidé en octobre 2020 à travers l'arrêt « French Data Network et autres »[49] les textes européens – et, par ricochet, les législations nationales – qui régissaient depuis 2002 en Europe (et 2001 en France) la conservation et les réquisitions judiciaires et administratives des « données de trafic » générées par l'usage des services des fournisseurs d'accès à Internet, des opérateurs de télécoms et des prestataires d'hébergement. Certains se réjouissent que l'exigence de proportionnalité et de transparence des lois sécuritaires ait enfin prévalu sur des équilibres « sécurité/libertés » jusqu'à présent dégagés par des majorités parlementaires placées sous le contrôle de leurs cours constitutionnelles. D'aucuns pointent le paradoxe qui consiste à ne pas soumettre au droit européen les politiques de sécurité publique, mais de les déconstruire *a posteriori* par la jurisprudence de la CJUE inspirée de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales de 1950.

Cette judiciarisation ne construit pas une puissance, ni une croissance européenne. Par ailleurs, l'inspiration indéniable du droit européen est réinterprétée par des souverainetés étrangères érigées pour faire échec au droit européen. Par exemple, la nouvelle loi chinoise PIPL *(Personal Information Protection Law)* entrée en vigueur le 1er novembre 2021 établit un corpus puissant de règles se présentant comme participant du consentement individuel du citoyen – inspiré du RGPD – et articulé à l'autorisation administrative préalable et à l'obligation de localisation en Chine des serveurs et des données, montrant qu'on peut être imité par des stratégies opposées à nos objectifs ou nos valeurs. Ces initiatives interrogent l'Union européenne, dont la puissance ne paraît se matérialiser que par le droit issu des contentieux dont sont saisies ses juridictions suprêmes, au gré d'intérêts circonstanciels et catégoriels.

49 Arrêt du 6 octobre 2020, Affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e. a. contre Premier ministre e.a. : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62018CJ0511

Ce pouvoir de régulation de l'économie numérique est lui-même limité et peine à faire émerger une souveraineté technologique. L'Union européenne est une entité politique qui s'est bâtie autour de questions intimement liées à la régulation des marchés et au droit de la concurrence, et qui se heurte désormais en matière de souveraineté technologique à un Internet en partie privatisé et oligopolistique. Si cet enjeu concerne toute grande puissance qui doit aussi repenser ses régulations, ce défi revêt des formes spécifiques pour l'UE. Son architecture juridique la contraint elle-même dans son pouvoir de régulation. À ce titre, le professeur Théodore Christakis rappelle le frein que constitue le vote à l'unanimité qui rend souvent difficile la possibilité d'obtenir un accord entre les États membres. Cela était le cas pour les débats sur la taxation des services numériques, la fiscalité étant un champ où l'unanimité est requise. L'universitaire souligne que cette difficulté se pose également sur des décisions fondées sur la majorité, prenant l'exemple du règlement *E-evidence*.[50]

Au-delà des procédures de vote, la souveraineté technologique de l'Union européenne est freinée par le fait que la sécurité nationale demeure une prérogative des États membres.[51] Tous les États membres n'en ont d'ailleurs pas la même conception. En matière numérique, il y a, par exemple, des différences de conception sur le traitement de données liés à la sécurité des États, notamment sur le contrôle qui doit en être fait. Sur ce point, Théodore Christakis considère que la série de jugements de la Cour de Justice de l'Union européenne du 6 octobre 2020 qui concernent l'accès des gouvernements aux données de communication a participé de l'érosion de l'exemption sur la sécurité nationale.[52] Cependant, si cette jurisprudence a affaibli les souverainetés nationales en imposant aux États membres le respect des critères du droit européen des droits de l'homme, elle n'a pas pour autant renforcé la souveraineté européenne. Paradoxalement, l'immixtion du droit européen dans les stratégies nationales de sécurité a pour effet immédiat de dissuader les velléités d'une construction européenne de la sécurité.

50 Christakis, T., *op. cit.*

51 Il existe une limite légale à ce que l'UE puisse exercer son pouvoir de régulation sur les enjeux de sécurité nationale. Selon l'article 4(2) du Traité de l'Union européenne, « *L'Union respecte [...] les fonctions essentielles [des États membres], notamment celles qui ont pour objet [...] de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.* »

52 T. Christakis, *op. cit.*

Les débats qui traversent actuellement l'Union européenne montrent plus généralement que tous les États membres n'ont pas la même approche (et parfois le même respect) de l'État de droit. Les liens en matière de sécurité entre les États membres et les États tiers relèvent ainsi souvent de relations bilatérales et peuvent diverger entre États membres. Ces divergences ont été rappelées par la chercheuse Marietje Schaake lors de la conférence européenne organisée par Renaissance Numérique en mai 2021 sur la souveraineté numérique européenne : « *Ces deux domaines* (le marché unique européen et la sécurité nationale) *sont actuellement en conflit l'un avec l'autre : il y a la promesse d'un marché unique du numérique en Europe, mais il y a vingt-sept autorités différentes pour évaluer si la sécurité nationale est en jeu. Cet aspect a été souligné lorsqu'elles ont dû examiner si les technologies de Huawei et d'autres technologies de réseau étaient suffisamment sûres pour être utilisées en Europe.* »[53]

Cet enjeu est intriqué dans celui de la politique de défense commune qui peine à être construite par manque d'une vision partagée de la puissance de l'Union européenne. Si l'UE n'est pas capable d'avoir un projet de défense commune, il lui sera difficile d'avoir un projet de souveraineté – que cette défense et cette souveraineté soient numériques ou non. L'influence forte des États-Unis au travers de l'Organisation du Traité de l'Atlantique Nord (OTAN) en Europe joue à ce titre un rôle significatif dans cette contrainte, à l'heure où la maîtrise des câbles sous-marins présents dans les eaux territoriales françaises dépend de discussions au sein de son enceinte[54].

53 Renaissance Numérique (2021), "Digital Sovereignty: Which Strategy for Europe?" : https://www.renaissancenumerique.org/publications/digital-sovereignty-which-strategy-for-europe

54 « L'OTAN veut protéger les câbles sous-marins des attaques russes », Euractiv, 23 octobre 2020 : https://www.euractiv.fr/section/politique/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

UNE SOUVERAINETÉ TECHNOLOGIQUE QUI NE PEUT ÊTRE QU'EUROPÉENNE ?

Il convient désormais de dépasser ces freins, car la souveraineté technologique ne peut exister pour les États membres sans être européenne. Pour des raisons de capacité d'investissement, il n'y aura de souveraineté technologique qu'à l'échelle communautaire. Dans ce contexte, l'Union européenne doit être considérée comme un levier de puissance pour les États membres.[55]

Dès lors, il s'agit de faire prévaloir le principe de subsidiarité inscrit dans le droit de l'Union européenne. Comme le rappelle le Parlement européen, « *il* [le principe de subsidiarité] *ne légitime l'exercice par l'Union de ses pouvoirs que lorsque les États membres ne sont pas en mesure de réaliser les objectifs d'une action envisagée de manière satisfaisante et que l'action au niveau de l'Union peut apporter une valeur ajoutée* »[56]. L'Union européenne a vécu trop longtemps dans le déni des questions de puissance. Des États membres sont d'ailleurs opposés à une Union puissante. Or, si les États membres souhaitent garantir leur propre souveraineté technologique, ils doivent accepter le principe de subsidiarité en ce domaine. Ce dernier ne nie pas leur souveraineté nationale. Il est permis par leur état de souveraineté et se traduit par une répartition de compétences.

En cela, l'histoire européenne du spatial doit inspirer. L'autonomie d'accès à l'espace a, dès l'origine, été considérée comme un élément de souveraineté par d'importants pays de l'UE. Par la suite, le projet Galileo a été défini et mis en œuvre parce que les clés de dégradation du signal, synchronisation, datation et localisation GPS étaient détenues par le Pentagone américain. L'histoire récente du spatial peut également servir d'analyse éclairante. Alors que de nouveau acteurs d'origine privée montent en puissance, à l'instar d'opérateurs comme SpaceX, dirigé par Elon Musk, l'ouverture des appels d'offres par l'État américain, qui en garde donc la maitrise, leur profite directement.

55 Assemblée nationale, *op. cit.*

56 Voir sa présentation sur le site du Parlement européen : https://www.europarl.europa.eu/factsheets/fr/sheet/7/le-principe-de-subsidiarite

CONCLUSION
L'UE DOIT PENSER LE COUPLE « PUBLIC/PRIVÉ » DE MANIÈRE STRATÉGIQUE

Si les États membres souhaitent garantir leur souveraineté technologique, cette dernière ne peut être qu'européenne. Il ne s'agit pas de renoncer à leur souveraineté nationale, mais au contraire de la renforcer en s'en donnant les moyens collectifs. Pour cela, il est primordial de sortir de la confusion des termes, qui ne permet pas d'avoir une vision claire et commune des objectifs pour l'Union européenne.

Le numérique est une dimension stratégique par laquelle il s'agit de transiter pour redéfinir le territoire d'exercice de la souveraineté classique. Il s'agit donc d'établir les conditions d'accès à cette dimension. Pour ce faire, il convient d'analyser en profondeur les différentes couches technologiques du numérique et de déterminer quels sont les seuils critiques en dessous desquels la souveraineté technologique européenne n'est pas assurée.

Les États-Unis ont développé une approche stratégique de l'économie avec les « autoroutes de l'information » (*Information Superhighway*) sous l'ère de Bill Clinton et l'adaptation au numérique du *Foreign Intelligence Surveillance Act* (ou FISA) de 1974, qui inclut dans sa définition de la souveraineté nationale la puissance et les intérêts économiques au service de la puissance nationale, en particulier dans les rapports internationaux.

Cette conception économique de la *"national security"* américaine a plus d'un demi-siècle. Elle se traduit par des convergences d'intérêts public-privé valorisées. Son expression au service d'intérêts économiques et stratégiques considérés comme « souverains », est autant réglementaire, judiciaire, diplomatique, qu'économique et ne s'est jamais cantonnée au pré-carré supposé régalien de la défense et de la sûreté nationales, ni au seul territoire géographique américain. Du *Small Business Act* de 1953 – qui incarne l'affirmation économique d'une préférence nationale dans les secteurs émergeants – à l'instrumentalisation du droit et du juge à des fins de puissance économique et stratégique, de la lutte anti-corruption et anti-blanchiment, au contrôle des transactions en dollars et des investissements étrangers, en passant par les politiques d'embargo, l'arsenal juridique et judiciaire américain s'assume résolument comme un instrument de projection extra-territoriale de la puissance économique et politique, destiné à défendre et promouvoir les intérêts des États-Unis à l'international. Cet arsenal est constitué d'une chaîne de compétences économiques qui irriguent profondément l'organisation judiciaire,

diplomatique et régalienne de l'État fédéral, bien au-delà des régulateurs économiques apparents[57].

Avec des cultures politiques et des méthodes différentes, la Chine et la Russie ont, elles aussi, décidé depuis une quinzaine d'années d'instrumentaliser le cadre de développement de leurs hôtes économiques et stratégiques, en recourant à une approche très maîtrisée des intérêts stratégiques et régaliens – offensifs et défensifs – de la puissance technologique.

Ainsi, la capacité d'une puissance locale ou régionale à exporter ses technologies est un moyen d'assurer non seulement sa souveraineté technologique, mais également un levier de puissance à l'égard de ses interlocuteurs internationaux.

Alors que l'objectif de souveraineté technologique impose des investissements massifs et rapides, il est plus que jamais nécessaire que l'UE se dote d'une approche convergente qui dicte les agendas politiques et économiques. Or, jusqu'à l'année 2019, l'imbrication des enjeux économiques et technologiques n'était pas pensée en termes de souveraineté européenne, pas davantage qu'au niveau des États membres.

L'un des facteurs pouvant expliquer ce déficit de vision puis d'action n'est pas tant lié à une question de compétence, qu'à celle de la méthode, résultant elle-même d'une culture politique, judiciaire et administrative. La conception du rôle de l'action publique au service de ces enjeux stratégiques a très souvent confiné l'« État-stratège » à un rôle de bailleur de fonds publics ou de régulateur des excès de la puissance économique au sein du marché intérieur. Il aura fallu attendre les premiers discours de Thierry Breton, commissaire européen au marché intérieur et l'impulsion du programme *Digital Compass for 2030*[58] pour voir s'incarner depuis 2019 une vision politique du déficit de puissance européenne dans les secteurs technologiques. La pandémie mondiale a offert à cette impulsion une consolidation et un élargissement idéologiques.

Toutefois, l'Union européenne, tout comme la plupart de ses États membres, ne parvient pas encore à s'affranchir d'une conception administrative et judiciaire du rôle de la puissance publique, mêlant une théorisation rigide de ce qu'il incombe à « l'État » de faire ou de ne pas faire et un réflexe de relative méfiance à l'égard des acteurs privés. Cette conception encore dominante puise profondément ses racines dans les cultures nationales et européenne de la puissance, qui peut être résumée ainsi : si elle est publique, la puissance devrait être indépendante des intérêts économiques ; si elle est privée, elle devrait être réduite dans ses excès.

Sur le fond, ces deux terrains d'expression d'une défiance relative à l'égard de la puissance économique, freinent encore l'avènement d'une méthode partenariale de la puissance européenne, qui devrait nécessairement mêler des intérêts et des acteurs publics et privés. Pour ce faire, il s'agirait pour les pouvoirs publics d'admettre qu'ils devraient davantage profiter du point d'observation des affrontements économiques que leur conférerait la multiplication de leurs échanges avec les acteurs économiques, au-delà de la pratique punitive – judiciaire et administrative – du droit. Si cette ouverture méthodologique se confirmait, la pertinence des politiques publiques s'en trouverait nécessairement renforcée.

Il s'agit également pour les acteurs économiques européens d'avoir davantage confiance dans la protection diplomatique que leur offre le droit européen hors des frontières physiques du territoire de l'Union européenne. Une telle confiance ne se décrète pas. Elle s'obtient par des actes législatifs, administratifs, diplomatiques et judiciaires et non par des discours, si volontaristes soient-ils.

L'UE doit désormais – comme le reste du monde – concevoir ses compétences économiques, judiciaires et administratives dans une dimension stratégique et articuler l'indépendance de ses régulateurs sectoriels et transverses avec l'affirmation de ses objectifs stratégiques.

La souveraineté est toujours imparfaite[59], puisque sa nature est d'être contestée au gré de rapports de force permanents. Il en est de même avec la souveraineté technologique, contrainte par les interdépendances inhérentes à la production des technologies. Mais la souveraineté doit être une affirmation permanente, car elle ne se partage pas.

57 Voir à cet égard : Pierucci, F., Aron, M. (2019), *Le piège américain*, JC Lattès.

58 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *op. cit.*

59 Selon l'expression de Stephen Krasner citée par : Pohle, J., Thiel, T. (2020), "Digital sovereignty", Internet Policy Review, 9(4). Accessible via https://doi.org/10.14763/2020.4.1532 et https://policyreview.info/concepts/digital-sovereignty

REMERCIEMENTS

NOUS REMERCIONS POUR LEUR CONTRIBUTION, LES DIFFÉRENTS ACTEURS QUI ONT PARTICIPÉ AUX AUDITIONS, À SAVOIR :

Daniela Battisti, Directrice des relations internationales, Ministère de l'Innovation technologique et de la Transformation numérique, Italie

Godefroy Beauvallet, Chef du service du Conseil général, Conseil général de l'économie

Annie Blandin, Professeure, Département « Systèmes réseaux, Cybersécurité et Droit du numérique », IMT Atlantique

Christine Cabuzel-Duvallon, Adjointe, Secteur « Marché intérieur, industrie, recherche et innovation, numérique, espace », Secrétariat général des affaires européennes

Joffrey Célestin-Urbain, Chef du service de l'information stratégique et de la sécurité économiques, Ministère de l'Économie, des Finances et de la Relance

Vice-amiral Arnaud Coustillière, Cyber and Digital Senior Advisor, Str@t-Algo

Raphaël de Cormis, Vice-président "Digital Factory", Thales

Stéphane Dupuis, Secrétaire général adjoint des affaires européennes, Secrétariat général des affaires européennes

Laurent Ferrali, Directeur de l'engagement des gouvernements et des OIG, ICANN

Nico Geide, Policy planner for digital issues, Ministère des Affaires étrangères, Allemagne

Thibaut Kleiner, Directeur « Stratégie et diffusion des politiques », DG CNECT, Commission européenne

Olaf Kolkman, Principal "Internet Technology, Policy, and Advocacy", Internet Society

Konstantinos Komaitis, Senior Director "Strategy and Policy Development", Internet Society

Stefan Koreneef, Conseiller Innovation, Science et Technologie, Ambassade des Pays-Bas en France

Tanguy Larher, Responsable Secteur « Marché intérieur, industrie, recherche et innovation, numérique, espace », Secrétariat général des affaires européennes

Henri Verdier, Ambassadeur pour le Numérique

Suzanne Yountchi, Economic Officer for Trade, Digital Economy and Cybersecurity, Ambassade des États-Unis en France

RÉDACTION

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Etienne Drouard, Avocat associé, Hogan Lovells (Paris) LLP

MEMBRES DU GROUPE DE TRAVAIL

Guillaume Buffet, Président, U Change

Lucien Castex, Représentant pour les affaires publiques et le développement des partenariats, AFNIC

Arnaud Dechoux, Responsable des affaires publiques Europe, Kaspersky

Pierre-Frédéric Degon, Responsable des affaires gouvernementales, Abbott France

Hector de Rivoire, Responsable des affaires gouvernementales, Microsoft France

Etienne Drouard, Avocat associé, Hogan Lovells (Paris) LLP

Anne Duboscq, Directrice des affaires publiques, OVHcloud

Olivier Esper, Responsable des relations institutionnelles, Google France

Valérie Fernandez, Professeure et titulaire de la Chaire "Responsability for Digital IDentity", Telecom Paris

Henri Isaac, Maître de conférences, PSL Université Paris-Dauphine

Julie Lavet, Responsable des affaires gouvernementales, Apple France

Samuel Le Goff, Consultant, CommStrat

Emmanuel Lempert, Vice-président, Affaires publiques France, Afrique francophone et Moyen-Orient, SAP

Sophie Le Pallec, Responsable des affaires publiques, GS1 France

François Lhemery, Directeur délégué aux affaires publiques et à la communication, Numeum

Smara Lungu, Directrice « Marketing stratégique, veille concurrentielle et écosystèmes », Docaposte

Julien Nocetti, Chercheur associé, IFRI

Marine Pouyat, Consultante, W Talents

Jean-Luc Sauron, Haut fonctionnaire, Professeur, PSL Université Paris-Dauphine

Anne-Claire Wang, Responsable des relations institutionnelles, Huawei France

RELECTURE

Jessica Galissaire, Responsable des études, Renaissance Numérique

Henri Isaac, Maître de conférences, PSL Université Paris-Dauphine

Nous tenons également à remercier **Loane Bedouet** et **Pol-Euan Lacombe**, chargés de mission stagiaires au sein de Renaissance Numérique, qui ont accompagné le groupe de travail tout au long de ses réflexions.

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal *think tank* français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des *start-ups* et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la construction d'une société numérique inclusive.

RENAISSANCE NUMÉRIQUE

32 rue Alexandre Dumas - 75011 Paris
www.renaissancenumerique.org

JANVIER 2022

CC BY - SA 3.0