

La souveraineté numérique, un instrument de politique étrangère

Par Julien NOCETTI

Chercheur, GEODE (Géopolitique de la datasphère,
Université Paris 8) et IFRI

La pandémie de Covid est venue renforcer des tendances préexistantes : des interdépendances technologiques encore réelles, mais contrariées par la compétition entre les États-Unis et la Chine, et la problématique de la diversification des chaînes de valeur. La guerre en Ukraine, depuis février 2022, n'a fait qu'accélérer un mouvement global vers la prise en compte de logiques souveraines dans le champ numérique. Les États y agissent de façon naturellement différenciée en fonction de leur régime politique, suscitant des réponses et contre-réponses mêlant outils juridiques, financiers et technologiques. Instrumentalisée à des fins (géo)politiques, la souveraineté numérique est donc plus qu'une ambition industrielle – cette tendance devrait se renforcer à la faveur de la superposition des crises internationales.

Le champ numérique et, plus largement, technologique, est traversé de façon croissante par des logiques souveraines. La pandémie de Covid, la guerre en Ukraine, l'actualité juridique entre l'Union européenne (UE) et les États-Unis, mais aussi les choix d'investissements des plateformes numériques américaines et chinoises, participent à cette mise en lumière.

Dans un système international profondément travaillé par la dissémination globale des technologies numériques, certains États souhaitent s'appropriier les bénéfices de l'interdépendance technologique *lato sensu* tout en protégeant leur marché intérieur. La maîtrise des interdépendances est ainsi devenue un enjeu structurant des rapports internationaux, donnant un nouveau caractère d'urgence à des logiques de défense économique et commerciale.

La souveraineté numérique, par les rivalités qu'elle suscite, est également devenue un enjeu de modèle, de projection de valeurs politiques. Dans un monde marqué par le retour d'une forme de brutalisation, dans lequel le rôle des idées n'a jamais disparu, la souveraineté numérique apparaît comme une composante clé à travers laquelle les États en opposition voire en conflit viseront à porter leur propre lecture du droit, de la technologie et de la politique.

LA SOUVERAINÉTÉ NUMÉRIQUE DANS LA « CHAÎNE DE VALEUR » DIPLOMATIQUE

La souveraineté numérique est devenue l'un des points de friction désormais incontournable des rapports géopolitiques. Cette caractéristique a été clairement renforcée au cours de la crise pandémique puis à travers ses multiples implications. Deux d'entre elles méritent d'être relevées.

La première a trait à la montée en puissance du facteur géoéconomique dans les relations internationales, qui dépasse le seul cadre de l'économie numérique, pour englober des pratiques d'« arsenalisation » des principales interdépendances économiques. En d'autres termes, les vecteurs de la mondialisation (flux financiers, technologiques, exportations de matières premières agricoles et énergétiques, mais aussi réseaux informationnels) sont utilisés comme des armes. Selon cette approche, les mesures économiques coercitives – comme les sanctions – ne sont plus un substitut à la guerre mais son prolongement. L'objectif est d'assécher les ressources qu'un ennemi peut mobiliser pour le combat et donc d'alourdir le fardeau de la guerre à partir de la dimension économique. Il s'agit également d'affaiblir le moral de la population adverse afin de miner sa combativité et son soutien au gouvernement. Dans ce cadre, la souveraineté numérique peut constituer une réponse politique et industrielle à une situation de contrainte imposée de l'extérieur, dans une perspective d'« autosuffisance » (terme employé par les autorités chinoises depuis 2015) ou de « substitution aux importations » (vocabulaire utilisé par Moscou depuis 2014).

Dans le cas de la Russie, précisément, la souveraineté numérique ou technologique est depuis lors invoquée pour contourner les sanctions internationales, tout particulièrement dans l'industrie stratégique des semi-conducteurs, dans laquelle la Russie n'a pas de capacités de production propres (surtout les composants les plus sophistiqués), ni de chaîne de valeur souveraine. Le pays dépend principalement des architectures ARM pour les processeurs conçus par l'acteur national Baikal Electronics et de l'outil de production de l'entreprise taïwanaise TSMC. Toutes ces sociétés étrangères ont suivi les jeux de sanctions internationales, plaçant la Russie devant un risque de pénurie de composants, que le partenaire chinois n'est pas nécessairement enclin à prendre en charge, devant lui-même affronter les sanctions américaines visant ses approvisionnements en processeurs.

La seconde implication concerne les interactions entre les plateformes systémiques du numérique et les États. Ce sont les premières qui, pendant la crise du Covid, ont assuré les connexions entre pays, individus et organisations. Elles façonnent les rapports politiques et sociaux et sont désormais au cœur des rapports de puissance. La coopération, la compétition et la confrontation entre la Chine et les États-Unis se jouent notamment à travers elles. L'enjeu de la régulation des Gafam est de plus en plus perçu – en Europe tout particulièrement – comme celui devant permettre d'imposer une souveraineté numérique qui a longtemps fait défaut au continent. Elle se mue donc en un enjeu classique des relations internationales, susceptible, régulièrement, de déclencher des polémiques et de tendre les relations entre alliés (UE – États-Unis par exemple). Depuis 2019, l'Union européenne a fait de la taxation des Gafam l'un des axes politiques phares de sa « Commission géopolitique »¹. Les multiples initiatives communautaires en la matière sont désormais inscrites dans une volonté de défendre la « souveraineté numérique » de l'Europe face aux stratégies technologiques et d'innovation prédatrices des écosystèmes américains et chinois.

LA SOUVERAINETÉ NUMÉRIQUE, UN ENJEU DE MODÈLES

La souveraineté numérique ne représente pas qu'un enjeu de politique intérieure ; elle concerne également la projection d'une vision, d'un modèle à l'international. En la matière, une partie des débats actuels se focalise sur l'opposition de valeurs entre l'approche défendue par les démocraties libérales et celle projetée par les États autori-

¹ COMMISSION EUROPÉENNE (2020), *État de l'union 2020. La Commission von der Leyen : bilan de la première année*, https://ec.europa.eu/info/sites/default/files/von-der-leyen-commission-one-year-on_fr.pdf.

taires². Plus précisément, la ligne de fracture s'articule à un double niveau. Le premier concerne le degré d'ouverture d'écosystèmes numériques aux interdépendances globales – ou, du moins, à la capacité de ces États à maîtriser leurs dépendances critiques. Des régimes autoritaires comme la Chine, la Russie ou l'Iran visent, depuis la fin des années 1990 et à des degrés divers, à s'affranchir de leurs dépendances vis-à-vis des technologies américaines, perçues comme un moyen d'intrusion voire de subversion.

Le second a trait aux divergences d'appréciation même de l'expression de souveraineté numérique. Internet, défiant le contrôle de toute forme d'autorité, n'est pas unanimement perçu dans le monde comme devant à tout prix favoriser l'émancipation des peuples. C'est ici la couche cognitive de l'internet qui est concernée par cette approche. Distincte de la conception européenne, la souveraineté numérique telle qu'envisagée par la Russie ou la Chine met ainsi l'accent sur la préservation de l'espace informationnel « national » d'influences étrangères perçues comme subversives – tout en suivant les tendances internationales observées depuis une décennie (relocalisation des données, davantage d'importance accordée aux infrastructures numériques, etc.). Cette approche sino-russe se distingue également par un recours décomplexé au droit, mobilisé tous azimuts pour renforcer le primat du politique dans le domaine numérique et maintenir la stabilité – sinon la survie – des régimes. Dans les deux pays évoqués, la « sécuritisation » de l'espace numérique national s'est manifestée par l'emploi d'une rhétorique de la menace existentielle pour justifier des actions et des dispositions plus restrictives des libertés d'expression et de réunion. Une nouvelle fois, l'hostilité à la politique américaine – promotion de la liberté de circulation de l'information (*free flow of information*), rôle central du secteur privé, etc. – structure la ligne politique de ces États.

Cette forme d'autoritarisme numérique – intégrant une conception particulière de la souveraineté – est projetée de façon exponentielle dans les débats internationaux. D'une part, un État comme la Russie projette la notion de « souveraineté » ou de « sécurité » de l'information dans les enceintes internationales, tout particulièrement onusiennes, depuis 1998, cherchant à rallier les pays déjà américano-sceptiques à son propre positionnement³. Ligne de fracture dans les débats sur la gouvernance mondiale de l'Internet, la « souveraineté » est aussi exploitée par les mêmes États à des fins de politique étrangère. Ainsi, avant son interdiction dans l'Union européenne à compter de mars 2022, la chaîne d'État russe RT diffusait-elle, en France, des émissions et des articles pointant « l'absence » de souveraineté numérique en Europe, avec en contrepoint les différents scandales d'espionnage impliquant les alliés de façon à susciter des débats déjà polarisés au sujet des États-Unis.

Par-delà cette dichotomie liée à la nature des régimes, l'approche européenne se distingue, selon un nuancier complexe, par une ligne politique qui lui est désormais propre. L'absence d'acteurs numériques européens de premier plan conduit l'UE à défendre un modèle spécifique de société numérique autour de valeurs (protection des données personnelles, concurrence loyale, fiscalité suffisante...) dont la dimension défensive est parfois perçue comme une forme d'antiaméricanisme. En février 2021, Charles Michel, président du Conseil de l'UE, déclarait qu'il n'y a « pas d'autonomie stratégique sans souveraineté numérique », plaçant officiellement au cœur des débats le concept d'« autonomie stratégique », qui dénote une connotation sécuritaire voire militaire – ici appliquée à la politique numérique et aux infrastructures de données. Le curseur placé sur l'ambition d'« autonomie » suggère une lecture géopolitique devant permettre à l'UE de rivaliser avec les deux superpuissances numériques que sont la Chine et les États-Unis, tout en

² Voir par exemple WEBSTER G. & SHERMAN J. (2021), "The fall and rise of techno-globalism", *Foreign Affairs*, 28 octobre.

³ NOCETTI J. (2015), "Contest and conquest: Russia and global internet governance", *International Affairs*, vol. 91, n°1, pp. 111-130.

protégeant ses propres intérêts vitaux. Cependant, les États membres ne soutiennent pas tous le développement d'une autonomie stratégique européenne ; 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. L'attitude à adopter vis-à-vis des États-Unis est au cœur des discussions sur l'autonomie stratégique européenne et constitue l'un des points de crispation quant aux risques qu'elle pourrait faire peser sur les relations transatlantiques, particulièrement en matière de défense.

SOUVERAINETÉ VERSUS INTERDÉPENDANCES : L'EXEMPLE DE LA 5G

Pour les Européens, les débats sur la 5G sont venus questionner l'équilibre et l'avenir du rapport entre les interdépendances globales et les ambitions formulées de souveraineté ou d'autonomie stratégique en matière technologique. À cet égard, souveraineté numérique et souveraineté technologique sont souvent mêlées à propos de la 5G. Si la souveraineté numérique associe une longue liste de craintes (perte de contrôle des données, risques en matière de cybersécurité, rivalité numérique dans l'offre de services publics, menaces sur les libertés publiques et les valeurs démocratiques), la seconde recouvre la première mais se réfère plus globalement à la perte d'indépendance de l'Europe sur des technologies clés pour des secteurs stratégiques, comme l'industrie de défense et les infrastructures de télécommunications, ou pour l'avenir comme l'intelligence artificielle et l'Internet des objets (IoT).

Traditionnellement, deux lectures s'opposent lorsque la « souveraineté » de l'Europe est convoquée en matière technologique. Une première considère l'Europe « vassalisée », car dépourvue de capacité d'autonomie politique et économique sur ce plan. Une seconde avance, quant à elle, une croyance dans la capacité d'action de l'Europe dans le numérique et les technologies critiques, du fait de la formation d'une expertise scientifique de haut niveau et de la singularité d'un modèle de gouvernance fondé sur les valeurs européennes⁴. Ces deux lectures ne sont en réalité pas opposables : l'Union européenne sait tirer profit de son excellence technologique mais bute sur l'impensé géopolitique de son projet politique, qui se reflète parfois crûment dans le jeu technologique international.

Avec la 5G, l'évolution la plus notable concerne la question chinoise. Auparavant limitée à l'expansion des Gafam américains, l'ambition de souveraineté numérique de l'Europe est désormais décentrée des seuls États-Unis pour aussi englober la Chine. Cette donnée alimente un certain nombre de défis pour l'Union européenne et interroge autant son rapport à la mondialisation économique, centrée autour de la capacité productive de la Chine, que la nature « géopolitique » de la Commission telle qu'avancée dès son installation en décembre 2019 – soit en pleine phase de tensions transatlantiques. Ainsi, pour l'Europe, le dossier de la 5G témoigne jusqu'à présent de son absence de cohésion dans son rapport à la Chine de Xi Jinping. Diversement appréciée sur le continent, la compétition sino-américaine illustre pleinement la difficulté pour les Européens de déterminer leur positionnement commercial et stratégique par rapport à la Chine – et aux États-Unis – alors que s'affirme un « nationalisme technologique » que Pékin viserait à exporter⁵.

⁴ NOCETTI J. (2021), « L'Europe reste-t-elle une colonie numérique des États-Unis ? », *Politique étrangère*, n°3, pp. 51-63.

⁵ INKSTER N., *The great decoupling: China, America, and the struggle for technological supremacy*, Londres, Hurst, pp. 193-254. Pour une lecture du techno-nationalisme opposant les modèles politiques, voir WEBSTER G. & SHERMAN J. (2021), "The fall and rise of techno-globalism", *Foreign Affairs*, 28 octobre 2021.

La capacité de l'Union européenne à agir dans la sphère technologique, souvent reléguée au second plan dans les débats, pourrait être l'alpha et l'oméga d'une stratégie « en mouvement » du Vieux continent en matière de 5G. C'est une perspective qui semble se dessiner chez l'exécutif européen qui, en identifiant ses dépendances critiques dans des secteurs jugés stratégiques pour l'Europe, cherche à élaborer des mesures pour protéger les intérêts européens. En d'autres termes, la « souveraineté technologique » de l'UE serait mieux défendue en évaluant finement les dépendances critiques des États membres avant d'y répondre de façon ciblée tout en conservant une ouverture au monde⁶ plutôt qu'en adoptant une approche classique de la souveraineté, qui masque les logiques d'interdépendances qui restent les marqueurs de notre époque⁷.

CONTRER LA « FRAGMENTATION »

À l'échelle internationale, les logiques souveraines sont de longue date débattues sous l'effet supposé de celles-ci sur l'Internet voire le spectre complet du numérique et des technologies dites émergentes (intelligence artificielle, 5G, etc.). Une partie des débats place une emphase particulière sur le terme de « fragmentation », qui décrirait l'émiettement en cours du réseau global sous l'effet de politiques « souveraines », c'est-à-dire en contradiction avec la nature « globale, ouverte et interopérable » de l'internet des pères fondateurs. Il s'agit principalement de l'approche américaine, qui resitue l'enjeu dans une stratégie diplomatique visant à empêcher le morcellement de nos univers numériques à des fins politiques et commerciales⁸.

Cette « fragmentation » est parfois débattue à travers l'idée d'une sécession de certaines parties de nos réseaux. La « balkanisation », terme à la connotation négative, a été pour la première fois abordée dans une étude du MIT de 1997, laquelle prévenait que la croissance d'une infrastructure globale de communication ne conduirait pas nécessairement à l'émergence d'un « village global de l'internet » – elle pourrait aussi fragmenter les sociétés et « balkaniser » les interactions dans l'espace numérique⁹. Le « Splinternet », lui, désigne le fait d'avoir, en lieu et place d'un seul réseau mondial, des îlots numériques distincts, sans interopérabilité. Cela signifie que ces réseaux ne se parlent pas les uns les autres, voire même qu'ils opèrent sur des technologies différentes et incompatibles. Loin d'être accessoire, l'enjeu a pris un caractère géopolitique, la guerre en Ukraine ayant réveillé le spectre d'une fragmentation élargie. La Chine n'a pas le monopole de la fermeture de son réseau ; la Russie, elle, a renforcé son contrôle depuis l'invasion et bloque les grandes plateformes numériques. Dans ces cas précis comme ailleurs, la ligne de défense reste bâtie autour de la notion de souveraineté...

⁶ FIOTT D. & THEODOSOPOULOS V. (2020), "Sovereignty over supply? The EU's ability to manage critical dependencies while engaging with the world", EUISS, Brief, n°21, décembre 2020.

⁷ Sur le sujet, voir HÉRAULT P. (2021), « Comment renforcer la souveraineté à l'heure des chaînes de valeur mondiales ? », Études de l'Ifri, décembre.

⁸ Voir *Confronting reality in cyberspace: Foreign policy for a fragmented internet*, Independent task force report n°80, Council on Foreign Relations, 2022.

⁹ VAN ALSTYNE M. & BRYNJOLFSSON E. (1997), "Electronic communities: Global village or cyber Balkans?", Massachusetts Institute of Technology, mars.

BIBLIOGRAPHIE

COMMISSION EUROPÉENNE (2020), *État de l'union 2020. La Commission von der Leyen : bilan de la première année*, https://ec.europa.eu/info/sites/default/files/von-der-leyen-commission-one-year-on_fr.pdf

COUNCIL ON FOREIGN RELATIONS (2022), “Confronting reality in cyberspace: Foreign policy for a fragmented internet”, Independent task force report n°80, Council on Foreign Relations, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

FIOTT D. & THEODOSOPOULOS V. (2020), “Sovereignty over supply? The EU’s ability to manage critical dependencies while engaging with the world”, EUISS, Brief n°21, décembre, www.iss.europa.eu

HERAULT P. (2021), « Comment renforcer la souveraineté à l’heure des chaînes de valeur mondiales ? », *Études de l’Ifri*, décembre, www.ifri.org

INKSTER N. (2021), *The great decoupling: China, America, and the struggle for technological supremacy*, Londres, Hurst.

NOCETTI J. (2015), “Contest and conquest: Russia and global internet governance”, *International Affairs*, vol. 91, n°1, pp. 111-130.

NOCETTI J. (2021), « L’Europe reste-t-elle une colonie numérique des États-Unis ? », *Politique étrangère*, n°3, pp. 51-63.

VAN ALSTYNE M. & BRYNJOLFSSON E. (1997), “Electronic communities: Global village or cyber Balkans?”, Massachusetts Institute of Technology, mars, <https://web.mit.edu/marshall/www/papers/CyberBalkans.pdf>

WEBSTER G. & SHERMAN J. (2021), The fall and rise of techno-globalism, *Foreign Affairs*, 28 octobre, <https://www.foreignaffairs.com/articles/world/2021-10-28/fall-and-rise-techno-globalism>