

Territorialisation du cyberspace et géopolitique des GAFAM : facteurs d'influence et nouveaux risques à la faveur de la crise ukrainienne

Par Mohamed Benabid

PB -52/22

L'information constitue l'une des ressources les plus convoitées sur la planète, et invite à examiner la manière dont elle s'intègre en tant qu'objet de pouvoir et de domination dans les processus politiques, nationaux et internationaux. Les tensions autour de cette ressource s'expriment non seulement à travers les territoires directement contrôlés par les États mais aussi ceux disputés ou de compétition, y compris dans leur acceptation intangible comme pour le cyberspace. La guerre Russo-ukrainienne est emblématique de ces enjeux. Pour avoir « déconnecté » la Russie ou, au contraire, maintenu le service en Ukraine, la posture des GAFAM (acronyme qui renvoie aux géants du Web - Google, Apple, Facebook, Amazon et Microsoft), devenus parties prenantes dans le conflit et imposant une nouvelle image de leur puissance, a eu une forte consonance géopolitique. Ces développements pourraient renforcer un peu plus le sentiment de méfiance vis-à-vis du cyberspace et font résonner en filigrane le débat autour de la gouvernance d'internet et de cyber-souveraineté, des questions sur lesquelles les grandes puissances cherchent à se redonner des espaces stratégiques. Pour l'heure, l'enlisement du conflit éloigne un peu plus l'éventualité d'un scénario consensuel international.

Dès les premiers jours du déclenchement de la guerre Russo-ukrainienne, les GAFAM ont pris position se rangeant du côté du front pro-ukrainien qui a trouvé là un précieux auxiliaire contre Moscou, donnant au passage une nouvelle dimension aux conflits internationaux. Microsoft, Apple et Amazon ont ainsi suspendu la vente de produits, physiques et dématérialisés, en Russie à l'instar des applications du Play Store ou l'Apple Store, ou encore des services cloud AWS d'Amazon. YouTube a « suspendu » la génération de revenus publicitaires pour tous les médias d'État russes tandis que Google a déployé un système d'alerte aux bombardements sur son application Maps.

Au-delà de ces mesures physiques, le constat est celui d'une mobilisation sans précédent des réseaux sociaux pour continuer d'assurer leurs services en Ukraine. C'est ce qui a permis à Kiev de continuer de communiquer et de gagner une bataille de perception à l'international. Facebook, Instagram et WhatsApp ont même fait une entorse à leur règlement prohibant les appels à la violence, autorisant des formes d'expression politique qui en temps normal passeraient difficilement, comme pour « mort aux envahisseurs russes ».

CONFLICTUALITÉ GÉOPOLITIQUE

Ce n'est pas la première fois que des acteurs internet contribuent à une redistribution du pouvoir ou font vaciller les régimes en place. Au cours du printemps arabe, en 2011, à Hong Kong, pour les manifestations de 2019-2020, ou encore pour la première guerre d'Ukraine, celle du Dombass en 2014, le rôle joué par les réseaux sociaux numériques dans l'activisme et la mobilisation est établi. Plus récemment pendant la période Covid-19, ce rôle n'a fait que croître puisque la question des Gigatechs américaines s'est invitée au premier plan en interaction avec les enjeux de l'infodémie et avec en toile de fond le constat d'un écosystème informationnel très largement dominé par les GAFAM.

Si le fait de poser une partie du cyberspace en tant que lieu de conflictualité géopolitique n'a rien de radicalement nouveau en soi, la crise Russo-ukrainienne semble en décupler l'intensité dans la mesure où des entreprises de l'internet prennent frontalement position dans un conflit, cherchant à affaiblir l'une des fondations des stratégies de guerre, à savoir la maîtrise des flux d'information et de la communication. D'ailleurs, la guerre en Ukraine a montré que des configurations inédites pouvaient être envisagées avec la perspective de services complètement intégrés contrôlant toutes les composantes du cyberspace- comme pour le parcours d'Elon Musk à la fois opérateur télécom via Starlink et à un moment candidat à l'acquisition de Twitter avant de faire marche arrière sur ce projet de rachat. À rebours des premiers discours ayant accompagné les vocations originelles de ces entreprises, ces développements réaffirment la transition vers de nouvelles postures où les technologies s'affirment de plus en plus en tant qu'instrument de puissance. Souvent au service exclusif des plus gros. Si les GAFAM ne rechignent plus à se recouvrir de leurs nouveaux habits, c'est qu'ils sont confortés par leur suprématie technologique. Une force de frappe à chercher dans les fondations conceptuelles de la « société en réseau » au sens de Castell & Cardoso (1996)¹ ou dans les agencements complexes des « infrastructures de contrôle » pour reprendre la définition de Kumar (2021)², c'est-à-dire des « normes, conventions et modulations algorithmiques » qui vont contribuer à une régulation du « comportement humain sur le Web » (p.7).

1. Castells, M., & Cardoso, G. (1996). *The network society* (Vol. 469). oxford: blackwell.

2. Kumar, S. (2021). *The digital frontier: Infrastructures of control on the global Web*. Indiana University Press.

Cette puissance est corroborée par leur réussite financière : 2129 milliards de dollars de capitalisation boursière pour Apple³ (c'est plus que le PIB du Brésil, de la Corée ou du Canada), 1582 milliards de capitalisation boursière pour Microsoft, 1415 milliards de dollars pour Alphabet, maison mère de Google (presque le PIB de l'Espagne et plus que le PIB de l'Australie), 443 milliards de dollars pour Meta Platforms (Facebook).

COUCHE COGNITIVE

La raison d'être de ces entreprises peut interpeller sur des enjeux qui transcendent les aspects d'infrastructure physique, ou de « couches » pour reprendre un vocable du cyberspace. La typologie usuelle invite à ce propos à circonscrire les effets plutôt dans la couche dite cognitive ou informationnelle du cyberspace, celle qui concerne la production de contenu. Laquelle n'est pas désarticulée des autres couches : infrastructures, protocoles ou couche dite logique. Ce qui faisait cependant jusque-là l'exception s'installe désormais durablement dans le paysage faisant de cette couche du cyberspace, et à l'instar des trois autres, un lieu de rivalité.

Cette suprématie qui s'est renforcée au fil des ans fascine autant qu'elle inquiète. Quels garde-fous face à des groupes capables de connecter 4,6 milliards d'utilisateurs, soit plus de la moitié des habitants de la planète, mais en même temps trainent une réputation sulfureuse, soupçonnés ici de contrôler les systèmes par lesquels nous communiquons, là d'amplifier les contenus haineux, les fake news, là encore de maintenir dans une grande opacité les algorithmes au cœur de leurs modèles économiques.

Archétype d'un maillage informationnel mondial qui souvent nargue les cadres réglementaires, nationaux et supranationaux, et dont l'influence dépasse parfois le poids politique des États pour ce qui est de régir la vie démocratique et civique, ces entreprises raflent tout : l'essentiel du trafic, des recettes et de l'attention. Leur mainmise sur la manne des données personnelles crée qui plus est une asymétrie de pouvoir au détriment de l'utilisateur. Les esprits cyniques pourront toujours y trouver une belle vitrine du capitalisme digitalisé. Car à côté d'une version idéalisée d'internet qui a baissé les barrières d'entrée, qui a permis à de petits entrepreneurs de tenter leur chance, de devenir peut-être des influenceurs fortunés, il existe pour ainsi dire une image un peu plus nuancée, où les risques de concentrations sont importants, et profitent avant tout aux acteurs dominants et où les algorithmes ont désormais des relents géopolitiques.

CONCENTRATION

La concentration de pouvoir est ici problématique plus que tout autre secteur, tant elle charrie des enjeux de préservation ou de déstabilisation des démocraties. Même s'ils s'en défendent, ces groupes détiennent à l'instar des médias conventionnels, un pouvoir de « gatekeeping »⁴ de l'information et, partant, de formation des opinions publiques, de persuasion et d'influence. D'ailleurs, c'est pour cette raison que nous faisons résolument le choix dans le présent article de parler d'intermédiaire INTERNET ou d'infomédiaire⁵, les expressions mobilisées habituellement, « plateformes » n'étant pas neutre, associées parfois à une rhétorique discursive qui alimente une élasticité identitaire. Quand elle n'est

3. A la date 20 juin 2022

4. Cette notion, l'un des socles de la fonction journalistique, fait référence au processus de filtrage et de sélection de ce qui est publiable.

5. Terme désignant en l'occurrence des acteurs tiers assurant des effets de médiation entre un contenu numérique et des communautés humaines produisant et utilisant ce même contenu.

pas mobilisée pour camoufler le positionnement des acteurs ou à tout le moins à leur éviter toute critique ad hominem, laissant croire que ces entreprises n'ont pas de finalité éditoriale. Or c'est bel et bien autour de ces enjeux éditoriaux que tout se joue : la capacité d'influencer les masses, d'orienter ce que l'humanité consomme comme informations, d'accorder ou de retirer le droit à la parole. Non seulement la finalité éditoriale existe, mais plus problématique, les critères de curation (c'est-à-dire de sélection, d'édition et de partage d'un type de contenu) sont dissimulés, ce qui ne fait que renforcer le climat de suspicion.

Quant à leur statut géopolitique, il va au-delà et excède l'exercice conventionnel de territorialité et des formes de pouvoir, explicites dans le cadre des États. La nature de cette influence, politique, et le profil des acteurs, privés, invitent d'ailleurs à les garder comme fil conducteur pour les besoins de la présente analyse.

POUVOIRS SUBORDONNÉS

Comme s'en inquiète De Gregorio⁶, ce n'est pas tellement le pouvoir technologique ou algorithmique qui est interpellé, mais les « menaces provenant de la montée de pouvoirs privés transnationaux ». Plusieurs travaux ont étudié en quoi ces pratiques mériteraient les qualificatifs d'« internet anarchique », car fixées en interne, de manière discrétionnaire.

Reste à vérifier si cette puissance est le fait de pouvoirs subordonnés implicitement à un autre pouvoir, étatique cette fois-ci. Cette hypothèse, tenace dans une partie de la littérature considère que la distinction entre intérêts privés (ceux des GAFAM) et intérêts étatiques n'a pas lieu d'être, car les premiers ont dépendu à un moment ou à un autre de subventions publiques pour leur création ou développement. Pour la période contemporaine, personne ne peut, il est vrai, contester le rôle joué par l'administration Clinton à la fin des années 90 dans la stratégie de libéralisation d'Internet. Mobilisation qui sera incarnée à l'époque, notamment par le Vice-président Al Gore et son concept, devenu légendaire depuis, « d'autoroutes de l'information ».

Cette conception bourdieusienne du pouvoir ne peut cependant être validée sans réserve tant elle présuppose l'existence d'un agenda ancien (il faut remonter jusqu'aux années 30 pour identifier les premières structures américaines ayant donné le la sous l'impulsion de l'État entrepreneur de science) ou d'un ordre supérieur pour guider le processus.

Par indolence ou par crainte de compromettre les perspectives de développement de technologies au départ prometteuses, les pouvoirs publics dans de nombreux pays n'ont pas mesuré suffisamment la portée de ces transformations. Beaucoup assistent aujourd'hui impuissants à une déferlante qui vient les narguer dans leurs propres prérogatives, comme en témoigne le pouvoir de censurer un chef d'État (comme pour Donald Trump privé de compte Twitter en 2021)⁷, de faire ou de défaire des élections (à l'instar du scandale Cambridge Analytica et les soupçons de manipulation des données personnelles par Facebook), de connecter ou déconnecter un pays en prenant résolument position dans un conflit comme la guerre Russo-ukrainienne.

6. De Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

7. Bien qu'il faille reconnaître à ces entreprises l'ouverture d'espaces inédits de liberté d'expression, les manifestations de ce pouvoir sur les questions de modération de contenu ne s'accompagnent pas de garanties claires et transparentes pour la protection du droit des usagers.

DÉMONDIALISATION

Au vu de cette configuration inédite à l'échelle de la planète, il est permis de faire l'hypothèse d'une triple conséquence. D'abord, l'accélération du processus de territorialisation du cyberspace. Le nouveau contexte de tensions internationales a en effet accru les externalités négatives favorables au risque de démondialisation. Un sujet en débat depuis au moins la crise de 2008, si l'on se situe à l'échelle du taux d'ouverture du commerce international et qui aujourd'hui interpelle plus spécifiquement les télécommunications. On le sait, les stratégies de pont-levis surfent sur la montée du populisme et du nationalisme. Une tendance qui peut paraître paradoxale à l'ère de l'hyperconnectivité, mais qui trouve aujourd'hui un terreau fertile avec le bannissement par Moscou de Facebook, Twitter, Instagram ou Youtube ou dans le sens inverse par l'exclusion, par l'UE, de la principale banque russe, Sberbank, du système Swift, l'un des protocoles de communication majeurs du cyberspace.

Ensuite, conséquence de ce qui précède il faut s'attendre à ce que deux autres questions, celle de la gouvernance internet et celle de la cybersouveraineté soient de nouveau reposées. La première est inscrite sur l'agenda diplomatique depuis le sommet mondial pour la société de l'information, tenu à Genève en 2003 puis à Tunis en 2005. Charmée par les promesses du numérique, la gouvernance de l'internet est restée pendant longtemps le parent pauvre du constitutionnalisme, rythmé par les seules logiques du marché.

Puisqu'elle préconise habituellement l'autorégulation comme mécanisme de privilégié pour Internet, l'approche américaine a conforté ce statu-quo. Il s'agit d'une difficulté de taille qui tient à l'absence de consensus sur l'architecture juridique idoine, le paysage international dissimulant une réalité complexe entre les conceptions européennes romanistes du droit, et celle anglo-saxonne plutôt relevant du common law, où les normes émanent des pratiques et usages. D'ailleurs, dès le départ, la politique des pouvoirs publics américains a été celle du laisser-faire avec l'espoir d'une autorégulation qui n'est jamais intervenue finalement.

A ce fameux principe de l'Internet global, théoriquement indépendant du pouvoir politique, la Russie et la Chine opposent depuis des années un « internet souverain » ou les États devraient avoir leur mot à dire à travers des architectures à imaginer sous l'égide des Nations unies ou de l'Union internationale des télécoms (UIT). La question de l'ICANN (Internet Corporation for Assigned Names and Numbers), instance de gestion des noms de domaine longtemps restée sous domination américaine, va cristalliser dans un premier temps l'essentiel des discussions. En 2008, le débat refait de nouveau surface avec l'élection d'Obama, dont la victoire est attribuée, en partie, au recours massif aux réseaux sociaux et à l'exploitation des opportunités offertes par le Web 2.0.

CYBERSOUVERAINETÉ

Depuis 2010, l'importance croissante des médias sociaux va faire migrer le débat autour de la gouvernance d'Internet de la périphérie vers le centre, mais pas dans la direction souhaitée par la partie américaine fragilisée dès 2013 par les révélations d'Edward Snowden sur les systèmes d'écoute de la NSA (National Security Agency). Révélations qui auront l'effet d'une bombe et placeront les enjeux de la protection de la vie privée et des données personnelles au cœur de la matrice de ce que l'on peut appeler la « géopolitique d'Internet ».

La deuxième question, celle de la cybersouveraineté, n'est pas décalée de la première. La bataille fait déjà rage pour la maîtrise du lucratif marché de la data, devenu l'un des principaux terrains d'affrontement entre superpuissances, et des différentes applications de l'Intelligence artificielle. Le fait que les Gigatechs convoitent fortement l'infrastructure câblière sous-marine (détenue aux trois quarts par les GAFAM) va dans le même sens.

Dans une course à la sécurisation des approvisionnements, le bras de fer Sino-américain sur l'industrie des semi-conducteurs, ou plus récemment le « Chips Act, ou plan présenté par la Commission européenne en février 2022⁸ sont pareillement emblématiques de cette compétition. La suprématie américaine semblait jusque-là inattaquable. Mais pour combien de temps encore ? La volonté chinoise de faire mieux que les Américains est perceptible sur plusieurs fronts. Pékin nourrit l'ambition d'être au cœur de l'économie mondiale, à l'horizon 2049, anniversaire du centenaire de la Chine communiste, et pour y arriver mise sur ces technologies comme axe prioritaire de ce développement. Plus spécifiquement sur la thématique des réseaux sociaux, c'est surtout l'ascension fulgurante du Chinois TikTok, devenu en 2020 l'application la plus téléchargée dans le monde devant Facebook. Un succès qui passe mal sur le continent américain, Washington envisageant son interdiction sur les principales boutiques, Appstore, playstore, officiellement au motif que Pékin s'en servirait à des fins d'espionnage. Des attaques qui ne sont pas sans rappeler celles dont a fait l'objet un autre Chinois, Huawei. Valeur aujourd'hui, cette saga singulière place désormais son entrepreneur, Zhang Yiming, ainsi que sa maison mère, Byte Dance, dans les listes des Case studies prioritaires à étudier dans les business schools comme l'ont été Apple avec Steve Jobs, Tesla avec Elon Musk ou Facebook avec Mark Zuckerberg.

FABRICATION DES NORMES

Au cours de ces dix dernières années, la cybersouveraineté est devenue un enjeu majeur pour la Chine, Pékin ambitionnant non seulement de devenir une cyberpuissance, mais aussi de se placer dans la course à la fabrication des normes du cyberspace.⁹ Là, aussi, et comme pour la gouvernance d'internet, la Chine est favorable à un système égalitaire des chances où chaque État devrait avoir son mot à dire dans les processus de prise de décision des règles et normes qui régissent le cyberspace à l'échelle mondiale.¹⁰ C'est également la position de la Russie qui, à plusieurs occasions, a cherché à être le fer de lance d'un mouvement international qui donne la primeur aux gouvernements nationaux dans la fabrication des normes du cyberspace.

Les négociations autour du serveur DNS racine, l'architecture décisive qui permet la redirection de données via les noms de domaine (treize serveurs DNS racine existent) dans le monde, ont bien montré l'ampleur des enjeux. Pékin défend un cadre de négociation multilatéral, et non multipartite, de manière à réduire toute chance pour les États-Unis de garder le contrôle. D'autres terrains de compétition stratégique concernent la bataille autour de la 5G, de l'Internet des objets où Chinois et Américains cherchant à imposer leurs standards. Le vieux continent cherche aussi à imprimer son rythme à travers des initiatives qui cherchent à mettre à niveau le corpus existant autour de communs numériques, à l'instar des règlements Digital Services Act et Digital Market Act.

8. Celui-ci vise à multiplier par quatre les capacités de production européennes du continent d'ici à 2030.

9. Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, 1(1), 81-93.

10. Ibid

Le sujet contigu aux discussions sur la cyber-souveraineté porte sur le degré de responsabilité des États en cas de cyberincident à effets transfrontaliers, ainsi que le contrôle qu'ils sont censés exercer sur l'infrastructure se trouvant sur leur territoire.

Une partie de la doctrine occidentale considère, à ce niveau, que les règles s'appliquant au monde physique valent aussi pour cyberspace et qu'il suffit donc de les transposer. Cette orientation rejoint les recommandations du manuel de Tallin, guide publié en 2013 par un groupe de travail mandaté par l'Organisation du Traité de l'Atlantique Nord (OTAN) qui a adopté une interprétation extensive du droit international conventionnel sur la souveraineté.

Dans la foulée, la question de la souveraineté dans le cyberspace met le doigt sur une plaie toujours béante, celle du retard des pays en développement relégués au simple statut d'utilisateurs/consommateurs, mais qui gardent espoir de pouvoir s'insérer dans des négociations multilatérales. A condition que l'évolution du contexte politique et sécuritaire international n'en décide pas autrement.

Dans un monde qui restera, au moins à moyen terme, marqué par les affres de la crise Russo-ukrainienne, les chances d'un scénario optimiste sont faibles, mais existent tout de même. Elles supposent de considérer le cyberspace comme un bien commun international et, partant, à l'abri de tout contrôle souverain exclusif.

Conclusion

Le rôle géopolitique des GAFAM conserve une réelle pertinence pour analyser la guerre Russo-ukrainienne. S'il ne déplace pas fondamentalement le curseur sur l'issue des conflits, les guerres se gagnant d'abord sur le terrain, ce rôle pose des problématiques renouvelées dans l'histoire des relations internationales invitant à considérer des entreprises technologiques en tant qu'instruments de politiques étrangères sur lesquels les grandes puissances, et pas seulement les États-Unis, fondent leur suprématie, implicitement ou explicitement. L'irruption d'une composante numérique dans la guerre Russo-ukrainienne pourrait relancer la lutte pour l'hégémonie dans le cyberspace avec le risque d'accélérer sa territorialisation. Questionner ces enjeux suppose dès lors de rappeler les grands principes qui régissent les fondations d'internet, notamment sur les questions de gouvernance et de cyber-souveraineté et en explorant la nature résolument institutionnelle et politique des motivations et décisions des GAFAM. Puisqu'elles émanent d'acteurs non étatiques, dans la pure tradition des guerres hybrides, leurs pratiques font émerger des dilemmes juridiques et éthiques en raison de leurs effets transfrontaliers.

À propos de l'auteur, Mohamed Benabid

Mohamed Benabid est enseignant à la Faculté de gouvernance, sciences économiques et sociales (FGSES) de l'Université Mohammed VI polytechnique. Lauréat de l'École de journalisme de Strasbourg, titulaire d'un doctorat en sciences de l'information et de la communication de l'Université Paris VIII et d'un doctorat en science de gestion de l'ISCAE, il compte à son actif près de 30 ans d'expérience dans l'industrie des médias. Son parcours pluridisciplinaire l'a conduit à couvrir depuis plusieurs années un large éventail de sujets : veille et intelligence économique, Médias/journalisme, Knowledge Management, géostratégie d'entreprise, géopolitique, communication politique, gestion et communication de crise, entrepreneuriat, management stratégique, méthodologie de la recherche en sciences de gestion.

À propos de Policy Center for the New South

Le Policy Center for the New South: Un bien public pour le renforcement des politiques publiques. Le Policy Center for the New South (PCNS) est un think tank marocain dont la mission est de contribuer à l'amélioration des politiques publiques, aussi bien économiques que sociales et internationales, qui concernent le Maroc et l'Afrique, parties intégrantes du Sud global.

Le PCNS défend le concept d'un « nouveau Sud » ouvert, responsable et entreprenant ; un Sud qui définit ses propres narratifs, ainsi que les cartes mentales autour des bassins de la Méditerranée et de l'Atlantique Sud, dans le cadre d'un rapport décomplexé avec le reste du monde. Le think tank se propose d'accompagner, par ses travaux, l'élaboration des politiques publiques en Afrique, et de donner la parole aux experts du Sud sur les évolutions géopolitiques qui les concernent. Ce positionnement, axé sur le dialogue et les partenariats, consiste à cultiver une expertise et une excellence africaines, à même de contribuer au diagnostic et aux solutions des défis africains. [Read more](#)

Les opinions exprimées dans cette publication sont celles de l'auteur.

Policy Center for the New South

Building C, Suncity Complex, Al Bortokal Street Hay Riad 10100 - Rabat

Email : contact@policycenter.ma

Phone : +212 (0) 537 54 04 04 / Fax : +212 (0) 537 71 31 54

Website : www.policycenter.ma



THINK • STIMULATE • BRIDGE