# De la géopolitique derrière les données, des données derrière la géopolitique

Par **Amaël CATTARUZZA**
IFG, Université Paris 8

La multiplication des capteurs et des outils générant des données numériques dans notre vie quotidienne est devenue emblématique de notre époque. Avec le développement des objets connectés et l'émergence progressive de nouvelles technologies de communication comme la 5G, cette tendance va continuer de s'accroître dans les prochaines décennies. Aujourd'hui, malgré les réticences et les craintes qui s'expriment sur ces sujets, aucun des secteurs de nos sociétés n'est plus étranger à la numérisation, que ce soit dans les domaines de la santé, de la finance, de la gestion administrative, de l'enseignement, et même des loisirs. Cette tendance lourde à la mise en données de nos activités, processus que l'on peut désigner par le terme de « datafication », a pour corollaire une augmentation exponentielle des données numériques disponibles sur des phénomènes et des objets de plus en plus larges.

Aussi, il est impossible d'aborder la question de la géopolitique des données numériques sans interroger au préalable ce processus de datafication à l'œuvre, qui, loin d'être une démarche neutre, est d'abord un choix politique et stratégique. Les différences de point de vue entre les États sur la mise en données de certains secteurs, comme celui de la santé, ou sur les usages possibles des diverses données, ou encore sur la place des acteurs privés dans la gouvernance numérique, révèlent en creux de réels clivages culturels, politiques et géopolitiques. Or, ces divergences s'inscrivent dans un rapport de force international en termes de capacités numériques qu'il convient d'esquisser dans une seconde partie, avec une évolution qui semble aller d'une domination unilatérale américaine à l'émergence de puissances régionales affirmées, et une question centrale qui émerge concernant les modalités de souveraineté numérique des États. Par ailleurs, l'usage des données numériques a profondément transformé les modalités d'expression du pouvoir sur les territoires. Les frontières, objets traditionnels d'étude pour la géopolitique, en sont par exemple transformées.

## La datafication du monde : un processus politique et stratégique

Le terme anglais de « datafication » a été proposé en français par différents auteurs (Peres, 2015 ; Bastin et Francony, 2016 ; Cattaruzza, 2019) pour insister sur le caractère social de la mise en donnée du réel. En clair, l'acte de mettre en données suppose un choix humain préalable, ou plutôt une série de choix (quels phénomènes prendre en considération ? Par quelle méthodologie procéder ? Quelle technologie utiliser ? Etc.). En clair, la mise en données est un acte de création et de transcription, et la nature des données générées dépend en grande partie des choix effectués en amont. Cela peut paraître trivial, mais ce constat est le socle nous permettant de penser une géopolitique des données numériques. Cela induit qu'il n'y a pas de données qui soient complètement neutres et objectives. Chaque captation, chaque collecte, chaque traitement, impliquent une médiation humaine, qui présuppose des décisions reflétant un contexte social, économique, politique et géopolitique. Cette prévalence du social dans un processus qui semble conditionné par des dispositifs techniques avait déjà été pointée par Bruno Latour (Latour, 2007), et a été depuis lors plus largement explorée, entre autres, par Rob Kitchin (Kitchin, 2014).

Ce faisant, il est donc important de considérer la production, le transport, le stockage, le traitement ou la destruction des données numériques comme des décisions d'ordre stratégique, qui demandent

de prendre en considération, au travers des procédés techniques utilisés, tant les opportunités que les vulnérabilités engendrées. En ce sens, la géopolitique des données numériques ne se limite pas à l'étude des rapports de force existant à l'échelle internationale entre des acteurs puissants, qui disposent de ressources techniques avancées, et d'autres, plus dépendants, qui n'ont accès à ces ressources que par l'intermédiaire des premiers. De fait, elle offre un regard beaucoup plus large permettant d'appréhender les jeux d'acteurs à diverses échelles, que ce soit au niveau des individus, des entreprises, des États, ou de tout autre groupe constitué (Douzet, 2014 ; Douzet et Desforges, 2018). En ce sens, elle permet d'analyser les stratégies et les aspirations à l'œuvre derrière l'ensemble des pratiques numériques contemporaines, et d'inscrire ces dernières dans un contexte social. Du consommateur qui va choisir de commander son produit sur une plateforme américaine, plutôt qu'européenne ou chinoise, jusqu'aux attaques informatiques d'échelle mondiale, en passant par les pirates cherchant à hameçonner de nouvelles victimes, chaque relation entre acteurs au sein de l'espace numérique peut être analysée au travers d'un prisme géopolitique.

Néanmoins, considérer la datafication comme un simple vecteur de relations d'acteurs ne suffit pas à embrasser la complexité de ce phénomène. En effet, si les technologies numériques utilisées reflètent l'environnement social dans lequel elles sont déployées, elles le modifient en retour et génèrent de nouveaux espaces, de nouveaux territoires, de nouvelles modalités d'interaction entre les acteurs, de nouvelles formes d'expression du pouvoir. Le concept de code/espace formulé par Rob Kitchin et Martin Dodge, à la fin des années 2000, illustre en partie cette transformation globale de nos sociétés. Selon eux, le code/espace « se produit lorsque les logiciels et la spatialité de la vie quotidienne se forment mutuellement, c'est-à-dire se produisent l'un l'autre » (Kitchin et Dodge, 2011, p. 16). Les exemples de cette relation dialectique et fusionnelle entre le code et les espaces du quotidien ne manquent pas, des feux de circulation sur nos routes aux différents sas d'enregistrement dans les aéroports, en passant par l'usage d'instruments GPS, entre autres. Dans chacun de ces exemples, les données numériques deviennent des clefs qui vont influer directement sur les interactions homme/homme, homme/machine, et machine/machine dans les espaces considérés. Or, ces dispositifs posent question lorsqu'ils sont déployés dans des lieux à des fins de contrôle des populations : les espaces frontaliers, les champs de bataille, la cité… La géopolitique permet ainsi de s'interroger sur la manière dont les données numériques modifient les modalités d'expression du pouvoir sur des territoires.

## L'évolution de la géopolitique internationale à l'ère des données numériques

Les révélations d'Edward Snowden en juin 2013 concernant la surveillance de masse opérée par la NSA par les industries américaines du numérique ont mis à jour les conséquences de l'hégémonie américaine dans le domaine digital. Or, ces pratiques de surveillance demandent à être analysées autant par le biais des stratégies d'acteurs qu'elles ont révélées, qu'au travers de leur matérialité même, par le prisme des infrastructures techniques sur lesquelles elles reposent. Les recherches sur la couche basse du cyberespace, ou couche physique, ont montré que les technologies déployées dans la collecte de données, les lieux de déploiement, leur mode de transit, les infrastructures utilisées pour leur stockage et leur traitement, ne sont pas anodines et mettent en jeux des rapports de pouvoir, de dépendance et de domination (Douzet, 2014). De fait, l'espace numérique repose d'abord sur des infrastructures matérielles localisées et fait l'objet aujourd'hui de différentes formes de territorialisation. Au niveau physique, l'emplacement des datacenters répond à des critères géographiques et stratégiques précis (Bakis, 2013 ; Limonier, 2018) et peuvent être des enjeux de souveraineté pour les États (Bômont, 2018). Sur le plan logique, l'ensemble du code sur lequel repose l'espace numérique détermine son mode d'existence, ouvert ou fermé, discriminant ou non, visible ou caché (Lessig, 1999) et, par les biais des algorithmes de routage, il définit aussi les routes qu'empruntent les données, respectant ou non des logiques territoriales (Frénot et Grumbach, 2014). À cela s'ajoutent des dimensions politiques

(enjeux de gouvernance multi-latéraux ou multi-acteurs), économiques (concurrences industrielles dans les marchés du numérique), juridiques (diverses législations nationales et internationales sur les données) et symboliques ou culturelles (concurrence linguistique, diffusion idéologique, etc.). D'où l'incitation et l'engagement des pouvoirs publics dans de nombreux pays à développer des datacenters locaux, des câbles alternatifs, et des lois de protection sur les données permettant de faire contrepoids aux géants américains.

Cette évolution contemporaine est marquée par une nouvelle régionalisation de l'espace numérique, avec l'émergence de pôles régionaux qui concurrencent désormais les États-Unis au niveau local comme au niveau international. Les politiques industrielles de la Russie comme de la Chine illustrent bien ce constat. En Russie, la construction de « mega datacenters » en Sibérie a été entreprise en 2015 (Limonier, 2018). Ces investissements font suite à une loi adoptée par la Douma en juillet 2014 et entrée en vigueur en 2016, qui oblige les entreprises du numérique, quelle que soit leur nationalité, à stocker sur le territoire russe toute donnée concernant les citoyens de la Fédération. Ces initiatives russes révèlent une vision stratégique et économique de long terme, tant sur le plan interne (possibilité de conserver sur le territoire la manne économique générée par ces données) que sur le plan externe (possibilité d'étendre l'influence russe vers les pays de l'Asie centrale, qui pourraient y délocaliser une partie de leurs données). De son côté, la Chine, dans le cadre de l'initiative One Belt, One Road, a développé un projet de route de la soie numérique. D'importants investissements sont prévus en Asie, au Moyen-Orient, dans les Balkans ou encore en Afrique pour augmenter les capacités numériques de ces régions et y favoriser l'implantation durable des entreprises chinoises (Huawei, ZTE, Baidu, Alibaba, Tencent, Xiaomi). C'est un moyen de promouvoir les technologies chinoises dans divers secteurs clés, comme celui des *smart cities*, dans lequel le pays se projette comme l'un des leaders mondiaux.

Face à ces logiques de puissance et d'influence, la plupart des États s'interrogent aujourd'hui sur la forme que pourrait prendre une « souveraineté numérique » permettant de juguler les dangers économiques (destruction d'emplois, relation dissymétrique) et politiques (dépendance, espionnage, cyberattaques) que présentent ces nouveaux rapports de force. Or, si la souveraineté traditionnelle était définie par rapport au territoire, qui en constituait à la fois le socle et les limites, la souveraineté numérique, du fait de la nature réticulaire de l'espace numérique, pose de nouvelles questions. Celle-ci doit-elle passer par des politiques territorialisées (investissements dans des infrastructures nationales) ou plus globales (nouvelles juridictions comme le RGPD, loi de datalocalisation, etc.) ? À quelles échelles doit-on penser la souveraineté (échelle nationale ou régionale, comme dans le cas européen) ? Quels acteurs pourraient en être les artisans (acteurs étatiques et/ou industriels) ? Comment articuler cette recherche de souveraineté nationale avec une nécessaire coopération internationale pour faire face aux enjeux globaux (gouvernance, cybersécurité, cybercriminalité, stabilité dans le cyberespace, cyberguerre, etc.) posés par les réseaux numériques ? Quelles stratégies adopter dans un domaine où la confiance entre acteurs est fortement érodée avec la multiplication des cyberattaques et des pratiques de surveillance et d'influence ?

## Le pouvoir mis en données : le contrôle numérique des frontières

Aussi, comme pour la souveraineté, l'usage des données numériques a profondément transformé les modes de gouvernement et de surveillance des populations. Certains lieux comme les villes (*smart cities*) sont devenus emblématiques de ces changements opérés par la gestion numérique de tous types d'activités, dont les actions liées à la sécurité. De même, le cas des « frontières intelligentes » fournit une illustration de ces nouvelles pratiques de pouvoir que la géopolitique doit être en mesure d'étudier. Le fonctionnement des *smart borders* repose en grande partie sur la datafication des flux et l'interopérabilité de différentes bases de données. Celles-ci sont rendues disponibles aux agents de contrôle par un ensemble d'outils techniques disposés à la frontière,

de manière plus diffuse sur l'ensemble du territoire, ou encore embarqués par les agents – ce qui renvoie à la notion de « frontières mobiles » (Amilhat-Szary et Giraut, 2015). La mise en place de ces dispositifs, très coûteux pour les États, s'est accélérée après les attentats du 11 septembre 2001. De fait, ils sont présentés comme une solution technique et neutre permettant de trier les flux, tout en assurant la fluidité des circulations et en exerçant un contrôle quasi immédiat sur les mobilités ou les échanges considérés comme indésirables ou dangereux.

Dans le cas du contrôle de la frontière, cela impose une étude précise des instruments déployés et utilisés (clôtures *high-tech*, capteurs thermiques, sismiques, drones, satellites, etc.), qui de fait rendent possible une surveillance en-deçà et au-delà de la frontière, sur des zones de plus en plus étendues ; mais aussi une prise en compte plus large des lieux de stockage et de traitement des données, et des échanges internationaux qui sont faits de ces données. Ces dispositifs techniques ont amené à repenser l'architecture de sécurité à la frontière autour de quatre aspects : anticipation des flux, identification des flux par l'intermédiaire du *checkpoin*t (Ritaine, 2009) ou du point de passage (Graham, 2011), centralisation et mise en réseau des données (Cattaruzza, 2012). Ce faisant, la sécurité aux frontières passe d'un modèle régalien et exclusif caractérisé par des activités de renseignement national tenues en grande partie secrètes, à un modèle post-westphalien reposant principalement sur la coopération entre acteurs (États, agents de sécurité) et l'échange de données.

Il faut néanmoins relativiser cette sécurisation en réseau. De fait, les objectifs d'interopérabilité, et les idées sous-jacentes d'un contrôle omniscient, dans le cas des *smart borders*, sont plus des fantasmes que des réalités. Ainsi, le programme EUROSUR de l'Union Européenne – qui propose l'interopérabilité de plusieurs bases de données nationales (polices, marines, douanes, etc.) à l'échelle européenne – repose en réalité sur une multitude d'acteurs, dont les pratiques et les finalités sont en partie divergentes, ce qui limite son efficacité (Jeandesboz, 2017). Toutefois, bien qu'imparfaitement réalisées, ces nouvelles capacités de contrôle par les données donnent lieu à des adaptations juridiques, permettant, par exemple, l'arrestation de migrants illégaux sur des zones plus larges (comme dans le cas de la frontière entre les États-Unis et le Mexique), et à des coopérations internationales inédites (échanges d'informations entre agences de renseignement, accords autour du déploiement et de l'usage des technologies aux frontières, etc.). De fait, des pratiques de gouvernance sont en train d'apparaître, là où le contrôle des frontières reposait traditionnellement sur des logiques de gouvernement.

Néanmoins, ces pratiques suscitent également de nouvelles questions à la fois techniques (sécurisation des données, efficacité des technologies et des réseaux déployés, etc.), économiques (coût de ces dispositifs, de leur maintenance, de leur mise à jour, etc.), éthiques et politiques (respect de la vie privée, statut des personnes migrantes, intervention pour le sauvetage de migrants en danger, automatisation du contrôle, contrôle préemptif sur la base de profilage algorithmique, surveillance de masse alors que les personnes visées par le contrôle – migrants illégaux et terroristes – sont des groupes beaucoup plus étroits, etc.).

## Conclusion

À l'instar du géographe Halford Mackinder qui, au début du XX$^{e}$ siècle, voyait dans la révolution des chemins de fer un changement radical des relations stratégiques sur la scène internationale, il est nécessaire aujourd'hui d'analyser les modifications des relations et des rapports de force entre acteurs qu'amènent la numérisation et la datafication du monde. Nouvelles régionalisations, reformulation de la notion de souveraineté, renforcement des acteurs privés et non étatiques, nouveaux modes de gouvernement, de surveillance et de contrôle, les transformations en cours sont à la fois très diverses et profondes. Si, au niveau international, le paysage géopolitique peut paraître assez conventionnel à première vue (domination américaine, affirmation des puissances

russes et chinoises), les changements induits par le numérique sont sans doute plus importants que ceux induits par la révolution industrielle de la fin du XIX[e] siècle. Avec l'émergence d'acteurs privés dans les discussions internationales, et de nouveaux rapports aux individus et aux sociétés, nos conceptions éthiques et politiques, issues d'un ordre westphalien, sont aujourd'hui bouleversées.

## Bibliographie

AMILHAT-SZARY A.-L. & GIRAULT F. (2015), "Borderities: The Politics of Contemporary Mobile Borders", *in* AMILHAT-SZARY A.-L. & GIRAULT F. (eds.), *Borderities and the Politics of Contemporary Mobile Borders*, Palgrave Mac Millan, pp. 1-19.

BAKIS H. (2013), « Les facteurs de localisation d'un nouveau type d'établissement tertiaire : les datacentres », *Netcom*, 27-3/4, pp. 351-384.

BASTIN G. & FRANCONY J. M. (2016), « L'inscription, le masque et la donnée. Datafication du Web et conflits d'interprétation autour des données dans un laboratoire invisible des sciences sociales », *Revue d'anthropologie des connaissances*, 2016/4, vol. 10, pp. 505-530.

BÔMONT C. (2018), « Maîtriser le *cloud computing* pour assurer sa souveraineté », *in La Cyberdéfense. Politique de l'espace numérique*, TAILLAT S., CATTARUZZA A. & DANET D. (dir.), Armand Colin, pp. 91-98.

CATTARUZZA A. (2012), « La technologie révolutionne-t-elle la frontière ? Frontières et sécurité dans le monde contemporain », *Archicube*, décembre, pp. 49-56.

CATTARUZZA A. (2019), *Géopolitique des données numériques*, Paris, Le Cavalier Bleu.

DOUZET F. (2014), « La géopolitique pour comprendre le cyberespace », *Hérodote*, n°152-153, pp. 3-21.

DOUZET F. & DESFORGES A. (2018), « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *Netcom*, 32-1/2, pp. 87-108.

FRÉNOT S. & GRUMBACH S. (2014), « Les données sociales, objets de toutes les convoitises », *Hérodote*, 2014/1, n°152-153, pp. 43-66.

GRAHAM S. (2011), *Cities Under Siege: The New Military Urbanism*, Verso, 432 pages.

JEANDESBOZ J. (2017), "European border policing: EUROSUR, knowledge, calculation", *Global Crime* 18:3, pp. 256-285.

KITCHIN R. & DODGE M. (2011), *Code/Space. Software and Everyday Life*, Cambridge, The MIT Press.

KITCHIN R. (2014), *The Data Revolution*, Londres, Sage.

LATOUR B. (2007), « Pensée retenue, pensée distribuée », *in Lieux de savoir*, tome I, JACOB Christian (dir.), Paris, Albin Michel.

LESSIG L. (1999), *Code and other laws of cyberspace*, Basic books, 297 pages.

LIMONIER K. (2018), *Ru.Net. Géopolitique du cyberspace russophone*, Paris/Moscou, L'inventaire/L'observatoire, Centre d'analyse de la CCI France Russie.

PÉRÈS E. (2015), « Rapport CESE 2015 : les données numériques, un enjeu d'éducation et de citoyenneté », *Les avis du Conseil économique, social et environnemental*, n°2015-01.

RITAINE E. (2009), « La barrière et le checkpoint : mise en politique de l'asymétrie », *Cultures & Conflits* 73, printemps 2009, http://conflits.revues.org/17500