The geopolitics behind data, the data behind geopolitics

Amaël Cattaruzza,
IFG, Paris 8 University

Abstract:
The generalized use of digital data is more than a simple technical process. It has consequences that we should examine from a geopolitical viewpoint. For this purpose, "datafication" is described as political and strategic processes that require human decision-making in the current social and political contexts. International power relations thus come to light: digital power players and regional poles have emerged. Digital sovereignty has become a more urgent issue for nation-states. The general question thus crops up about how datafication has influenced the assertion of power, as in the case of "smart borders".

The proliferation in everyday life of sensors and other devices that generate electronic data has become typical of our times. Given connected devices and new forms of communications technology (*e.g.*, 5G), digitization is going to grow in the coming decades. Despite the hesitations and fears stimulated by it, no sector (not even health, finance, management, education or leisure activities) in our society is any longer a stranger to this process. This strong "datafication" trend will exponentially increase the electronic data available about an ever wider range of phenomena and subjects.[1]

The question of the geopolitics of electronic data cannot be broached without first examining datafication, a process that, far from being neutral, is, first of all, a political and strategic choice. Differences between nation-states — Which sectors (health?) are to be "datafied"? How may databases be used? What will be the place of private stakeholders in "digital governance"? — reveal cultural, political and geopolitical cleavages. These points of divergence are related to an international balance of power based on our digital capacities, the subject of the second part of this article. Since this balance is apparently shifting from unilateral domination by the United States toward the assertion of regional powers, a key question crops up about the digital sovereignty of nation-states. Meanwhile, the use of electronic data is deeply altering exercise of power over territories. Borders, a usual subject of study in geopolitics, have been transformed.

Datafication: A political, strategic process

Various authors have introduced the word "datafication" from English into French to refer to the social implications of putting reality into a set of data (PÉRÈS 2015, BASTIN & FRANCONY 2016, CATTARUZZA 2019). This action definitely implies that a human choice has been made (or rather a series of choices) about the phenomena to be taken under consideration, the methodology and technology to be used, etc. Datafication is clearly an action of creation and transcription. The nature of the data produced very much depends on choices made upstream. This remark, which might seem trivial, lays the basis for a geopolitics of electronic data. No data are completely neutral and objective. Each harvesting or collection of data, each processing of them, involves human

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in January 2021.

interventions, whence the presupposition that decisions have been made that are related to the social, economic, political and geopolitical context. Bruno Latour (2007) already pointed to this predominance of social considerations in a process apparently conditioned by technology. Since then, this aspect has been widely explored by others (in particular KITCHIN 2014).

It is important to take under consideration the production, transmission, storage, processing and destruction of electronic data and to examine the strategic decisions about these actions. This means that the technical procedures used must reckon with both the opportunities and vulnerability wrought by datafication. The geopolitics of electronic data does not just study power relations at the international level between the mighty who enjoy high-tech resources and the others who, more dependent, only gain access to such resources through them. This geopolitical vantage point provides us with a much broader view for understanding players' games at various levels, whether of individuals, firms, governments or organized groups (DOUZET 2014, DOUZET & DESFORGES 2018). In this sense, it helps us analyze the strategies and motivations underlying all contemporary pratices in digital technology and to place them in a social context. From the consumer who chooses to order products on an American (instead of a European or Chinese) platform to cyberattacks on a worldwide scale, not to forget the pirates out phishing for new victims, every relation between actors in the digital realm can be examined with the help of this geopolitical looking glass. Seeing datafication as a simple vector of relations between actors does not, however, rid this phenomenon of its complexity.

While digital technology reflects the social environment where it is put to use, it also modifies this environment and generates new spaces, new territories, new forms of interaction between players, and new ways for asserting power. The concept of "code/space" sheds some light on this global transformation of our societies: "*Code/space occurs when software and the spatiality of everyday life become mutually constituted, that is, produced through one another*" (KITCHIN & DODGE 2011, p. 16). There is no dearth of examples of this dialectical but "fusional" relation between code and everyday spaces, examples ranging from traffic lights to restricted areas in airports, not to forget our geolocation devices. In each of these examples, electronic data directly influence person-to-person, person-to-machine and machine-to-machine interactions. Questions crop up when such arrangements are implemented for the purpose of controlling people, as on borders, on battle fields or in cities. Geopolitics can help us examine how electronic data modify the ways in which power is exerted over territories.

International geopolitics during the era of electronic data

Edward Snowden's revelations in June 2013 about mass surveillance by the NSA and American high-tech firms exposed the consequences of US hegemony over the digital realm. This surveillance must be analyzed not only in relation to the strategies of the players implicated but also in relation to its material aspects, namely the technical infrastructure.

As research on the lower (physical) layer of cyberspace has shown, the technology used to harvest data, the places where it is deployed, the way data are transmitted, and the equipment used to store and process data are factors not to be overlooked, since they are the grounds of these power games, of these relations of dependency and domination (DOUZET 2014). In fact, cyberspace hangs on this material infrastructure, itself geolocated. This space has undergone various forms of "territorialization". At the physical level, precise geographic and strategic criteria are used to locate datacenters (BAKIS 2013, LIMONIER 2018). For nation-states, these centers can be stakes in a game of sovereignty (BÔMONT 2018).

A cyberspace depends on code, and all this determines its mode of existence: open or closed, discriminating or not, visible or hidden (LESSIG 1999). Via routing algorithms, code also determines the routes, which might or might not be geographically defined, for transmitting data (FRÉNOT & GRUMBACH 2014). To this are to be added other dimensions: political (multistakeholder or

multilateral governance), economic (competition between firms on the high-tech market), legal (national and international laws about data) and symbolic or cultural (rivalry between languages, ideologies, etc.). For these reasons and in an effort to counterbalance the American high-tech giants, public authorities in several countries are pushing for local datacenters, cables, etc., and for laws to protect data.

What characterizes this contemporary trend is the recent regionalization of cyberspace. In effect, regional poles are emerging that rival the United States locally and even internationally. The industrial policies of Russia and China are evidence thereof. In Russia, "mega-datacenters" are being built in Siberia (LIMONIER 2018), investments stimulated by a law that, adopted by the Duma in July 2014 and enforced in 2016, forces digital firms, regardless of their nationality, to store on Russian territory all data about the Federation's citizens. These Russian initiatives are evidence of a long-term, strategic, economic view both inwards (the possibility of keeping in the Federation the economic benefits derived from these data) and outwards (the possibility of exerting Russian influence on central Asian countries, which could outsource their data to Russia). As for China, its Belt and Road Initiative includes plans for an electronic equivalent of the Silk Road. Major investments are planned for Asia, the Middle East, the Balkans and even Africa in order to increase the digital capacities of these regions and support the durable installation of Chinese firms there (such as Huawei, ZTE, Baidu, Alibaba, Tencent or Xiaomi). Chinese technology will thus receive a boost in key sectors (*e.g.*, smart cities) where the country sees itself as a world leader.

Given this influence-peddling and power-seeking, most states now wonder what form of "digital sovereignty" would be able to contain the dangers — both economic (destruction of jobs, dissymmetry) and political (dependency, espionage, cyberattacks) — that stem from this new balance of power. Whereas sovereignty used to be defined in relation to a territory, which was both its grounds and border, digital sovereignty raises new questions. After all, cyberspace is made up of networks. Does digital sovereignty entail policies that are territorial (investments in national installations) or global (new jurisdictions, the GDPR, legislation about the location of data, etc.)? What scales are to be used for this sovereignty: national or regional (as in the case of Europe)? Who is to design this policy (state authorities and/or businessmen)? How to relate the quest for national sovereignty with the international cooperation needed to address the global issues of networks (governance, cybersecurity, cybercriminality, the stability of cyberspace, cyberwarfare, etc.)? Which strategies to adopt when ever more cyberattacks and cybersurveillance have seriously undermined trust?

Datafied power: Digital border controls

As in the case of sovereignty, the uses of electronic data have deeply altered methods of government and surveillance. Some places (*e.g.*, smart cities) symbolize the changes resulting from a digital management of all sorts of activities, including security. "Smart borders" are one example of these new practices of power that should be submitted to a geopolitical analysis.

Smart border operations depend very much on a datafication of flows and on the interoperability of databases. These databases are to be made available through installations at the border (or, less densely, throughout the national territory) and devices in the hands of security officers or on board their vehicles, whence the idea of "mobile borders" (AMILHAT-SZARY & GIRAUT 2015). This setup is onerous. Nonetheless, such arrangements, which have accelerated since the attacks of 11 September 2001, are presented as a neutral, technical solution for sorting flows while maintaining their fluidity and exerting a nearly immediate control over any movements or exchanges that are deemed undesirable or dangerous.

In the case of border controls, a detailed study must be made of the means deployed and used (high-tech fences, thermal sensors, drones, satellites, etc.) so that surveillance can be exercised on both sides of the border, in ever larger areas. Furthermore, there must also be places for storing

and processing data and for international exchanges of data. These technical requirements mean redesigning the architecture of border security around: on the one hand, the prediction of flows and their identification at checkpoints or gateways (RITAINE 2009, (GRAHAM 2011) and, on the other hand, the centralization and networking of data (CATTARUZZA 2012). Border security thus switches from being an exclusive prerogative of the state (which usually conducts activities of national intelligence in secret) to a post-Westphalian model mainly based on data exchanges and cooperation between states and their security officials.

Caveats about this networked security must be pointed out. The offer made by smart border programs (specifically, interoperability and omniscient control) is more phantasmal than real. The European Border Surveillance System (Eurosur) proposes an interoperability of several national databases (police, customs, etc.) on the European scale. However its effectiveness is limited by its reliance on a multitude of actors with practices and purposes that partly diverge (JEANDESBOZ 2017). Though imperfectly realized, these new offers of data-driven border controls have served as the basis for adjusting laws so as, for instance, to arrest illegal migrants (in a bigger area along the border between the United States and Mexico). They have also led to an unprecedented international cooperation, with information being exchanged between intelligence services and with agreements about deploying and using this border technology. In fact, practices of governance are appearing at points where border controls used to be based on a logic of government.

These practices raise questions that are technical (data security, the efficiency of the technology and networks used…), economic (the costs of equipment and installations, of their maintenance, of updates…), ethical and political (privacy, the status of migrants, rescue operations of migrants in danger, the automation of controls, preemptive controls based on algorithmic profiling, mass surveillance even though the persons targeted — illegal migrants and terrorists — are much fewer in number…).

Conclusion

Like the geographer Halford Mackinder who, at the start of the 20th century, saw the railroads as marking a radical change in strategic relations on the international level, we must nowadays analyze the changes in power relations and in the lineup of forces among the parties who are ushering in digitization and the datafication of the world. The changes are diverse but deep: regionalization, a reformulation of sovereignty, the empowerment of private, nongovernmental stakeholders, and new forms of government, surveillance and control. At first sight, the international geopolitical landscape might seem conventional: US domination while Russia and China assert their power. However the changes wrought by digital technology are very likely more important than those introduced by the industrial revolution at the end of the 19th century. On account of this emergence of private actors in international discussions and given the new relations with individual and societies, our ethical and political conceptions, derived from the Westphalian order, have been upended.

References

AMILHAT-SZARY A.L. & GIRAULT F. (2015) “Borderities: The politics of contemporary mobile borders” in A.L. AMILHAT-SZARY & F. GIRAUT (editors), *Borderities and the Politics of Contemporary Mobile Borders* (New York: Palgrave MacMillan), pp. 1-19.

BAKIS H. (2013) “Les facteurs de localisation d’un nouveau type d’établissements tertiaire: les datacentres”, *Netcom*, 27(3/4), pp. 351-384.

BASTIN G. & J.M. FRANCONY (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*, 10(4), pp. 505-530.

BÔMONT C. (2018) “Maîtriser le *cloud computing* pour assurer sa souveraineté” in S. TAILLAT, A. CATTARUZZA & D. DANET (editors.), *La Cyberdéfense. Politique de l’espace numérique* (Paris: Armand Colin) pp. 91-98.

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

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

DOUZET F. (2014) “La géopolitique pour comprendre le cyberespace”, *Hérodote*, 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*, 152-153, pp. 43-66.GRAHAM S. (2011) *Cities Under Siege: The New Military Urbanism* (London: Verso), available via https://libcom.org/files/Graham,%20Stephen%20-%20Cities%20Under%20Siege.%20The%20New%20Military%20Urbanism_0.pdf.

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, MA: MIT Press).

KITCHIN R. (2014) *The Data Revolution* (London: Sage).

LATOUR B. (2007) “Pensée retenue, pensée distribuée” in C. JACOB (editor), *Lieux de savoir: Espaces et commuanutés* (Paris: Albin Michel), pp. 605-616.

LESSIG L. (1999) *Code and other laws of cyberspace* (New York: Basic Books).

LIMONIER K. (2018) *Ru.Net. Géopolitique du cyberspace russophone*, (Paris: L’Inventaire).

PÉRÈS E. (2015) “Les données numériques, un enjeu d’éducation et de citoyenneté”, *Les Avis du Conseil Économique, Social et Environnemental*, report to the Conseil Économique, Social et Envrionnemental (CESE), n°2015-01.

RITAINE E. (2009) “La barrière et le checkpoint. Mise en politique de l’asymétrie”, *Cultures & Conflits*, 73, pp. 15-33, available at http://conflits.revues.org/17500.