Études de l'Ifri

EUROPE: SUBJECT OR OBJECT IN THE GEOPOLITICS OF DATA?

Thomas GOMART

Julien NOCETTI

Clément TONON

July 2018

ifri Institut français des relations internationales

The Institut français des relations internationales (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

This study has been carried out within the partnership between Capgemini and the Institut français des relations internationales (Ifri).

ISBN: 978-2-36567-924-4

The opinions expressed in this text are the responsibility of the authors alone.

How to quote this document:

Thomas Gomart, Julien Nocetti and Clément Tonon, "Europe: Subject or Object in the Geopolitics of Data?", *Études de l'Ifri*, Ifri, July 2018.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

About the authors

Thomas Gomart is Director of the French Institute of International Relations (Ifri).

Julien Nocetti is a Research Fellow at the French Institute of International Relations (Ifri).

Clément Tonon is a Foreign Affairs Adviser in the Senate.

Abstract

Data no longer should be understood as a sole commercial or regulatory issue, but rather as an actual stake of international politics. Mastering data is an issue involving different set of actors, with diverging motivations: it is a sovereignty and national security stake for states, a democratic stake for people (personal data), and a fundamental source of value creation for companies. For Europe, in a context of transatlantic tensions, the impact of the digital economy's center of gravity moving towards China is potentially significant. However, the General Data Protection Regulation (GDPR), adopted in May 2018, seems more of a regulatory, even ethical, answer to a geopolitical challenge. This report focuses on data localization as an essential, but not exclusive, component of a data policy. As such, it suggests a mapping of the main national data-related policies (United States, China, Russia, India, and Brazil), then it examines the European Union's answers while highlighting the geopolitical and geo-economics stakes, which should legitimately be taken into consideration.

Résumé

Les données ne doivent plus seulement être comprises comme un sujet juridique et commercial, mais comme un enjeu de politique internationale à part entière. La maîtrise des données fait intervenir des acteurs aux contours et aux motivations très différents : enjeu de sécurité et de souveraineté pour les États, elle est un enjeu démocratique pour les populations (données personnelles) et une source fondamentale de création de valeur pour les entreprises. Pour l'Europe, dans un contexte de vives tensions transatlantiques, les conséquences du déplacement du centre de gravité de l'économie numérique vers la Chine sont potentiellement significatives. Pourtant, le Règlement général sur la protection des données (RGPD), adopté en mai 2018, constitue davantage une réponse d'ordre réglementaire, voire éthique, à un défi de nature géopolitique. Cette étude se concentre sur la localisation des données comme composante essentielle, mais non exclusive, d'une politique de la donnée. Pour ce faire, elle propose une cartographie des principales mesures nationales en la matière (États-Unis, Chine, Russie, Inde et Brésil) et examine ensuite les réponses apportées par l'UE en soulignant les enjeux géopolitiques et géoéconomiques, qui devraient légitimement être pris en compte.

Table of Contents

Introduction

Adopted in April 2016 by the European Parliament, the General Data Protection Regulation (GDPR) entered into force in May 2018. This text aims to "give back to citizens the control of their personal data while simplifying the regulatory environment of businesses".[1] While its implementation within businesses and administrations raise many questions, it has also opened up a debate on data, a topic most often raised in terms of consumer interest and usage.

At the international level, the *doxa* in this topic, produced in particular by large corporate strategy consultancies, presents data as the new subject of economic activity – some presenting it as a kind of post-industrial oil – and its free flow as the condition of an inexorable convergence between globalization and digitalization.[2] Between 2005 and 2016, the volume of data flows was multiplied by 80, but *digital globalization* has been threatened by three types of policies: setting up of protectionist barriers, national standards on respect for privacy, and finally requirements for data localization.[3]

At the European level, awareness of the industrial disconnect in digital matters leads to a number of measures that seem more defensive than offensive. The ecosystem of the European Union (EU) has not succeeded in creating a digital "giant" capable of competing with the large American platforms (GAFAM)[4]. In parallel, in China the rise of platforms (BATX)[5] benefiting from a protected domestic market can be seen. The absence of leading European digital players leads the EU to defend "a specific digital society model around values (protection of personal data, fair competition, sufficient taxation, etc.) whose defensive dimension is sometimes perceived as a form of anti-Americanism".[6] The Junker Commission has made the single digital market one of its main objectives, notably by favoring the free flow of non-personal data within the EU in order to spur innovation. A reaction to the Snowden disclosure, which saw the previous transatlantic data transfer agreements questioned (*Safe Harbor* then *Privacy Shield*),

1. European Council, "The General Data Protection Regulation", April 11, 2016.
2. McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows*, March 2016.
3. S. Lund and J. Manyika, "Defending Digital Globalization", *Foreign Affairs*, April 2017.
4. Google, Apple, Facebook, Amazon and Microsoft.
5. Baidu, Alibaba, Tencent and Xiaomi.
6. X. Merlin and M. Weill, "Quel avenir numérique pour l'Europe ?" [What is Europe's Digital Future?], *Réalités industrielles*, February 2018, p. 44.

the establishment of the GDPR is fundamentally aimed at regulating and protecting data exchange between European citizens and the GAFAMs, who have been well prepared for its implementation.

In France, the media debate on data has been partly on the question of their ownership.[7] In September 2014, the function of Chief Data Officer was created to design a policy for data produced or used by the government, around three main axes – supply, circulation and use – in order to improve the effectiveness of public action (in a rationale of *open data*). Promulgated in October 2016, the "law for a Digital Republic" aimed to "give France a head start in the digital field by favoring a policy of opening up of data and knowledge".[8] The law is organized around three axes: circulation of data, protection of individuals and digital access for all.

Protection and control of data is also a matter of defense and security policies. By definition, these are conceived in a national context in relation to the provisions implemented by other States to protect their own data or to appropriate those of others. Three recent documents have clarified the national/international articulation: in December 2017, France's *International Digital Strategy*; in February 2018, the *Cyber Defense Strategic Review*; in March 2018, the Villani report, *Giving Meaning to Artificial Intelligence. For a National and European Strategy*. The first document recalls that "the European Union must lead an active policy for promotion of its high standards of personal data protection" and that "France defends the establishment of a European observatory for platform transparency".[9]

The second document notes American leadership in cyber defense, while emphasizing "the problem of the private sector's acceptability of State interventions in information systems security". It also notes that in countries such as China and Russia, "the government must not only ensure the integrity of its networks but also control the content of the information that passes through it. This approach is in fundamental opposition with the Western conception of cyberspace".[10]

7. See for example, Génération Libre, *Mes data sont à moi, Pour une patrimonialité des données personnelles* [My Data Are Mine, for Ownership of Personal Data], January 2018.
8. Law N° 2916-1321 for a Digital Republic, October 7, 2016.
9. *Stratégie internationale de la France pour le numérique* [France's International Digital Strategy], presented by Mounir Mahjoubi and Jean-Yves le Drian, December 2017, part II.1. Also note this passage: "In addition, international transfers outside the European Union of personal data are in principle prohibited unless waivers are provided (in particular where the destination country provides an adequate level of protection). The protection of personal data must be excluded from the scope of international trade negotiations in order to preserve the application of European rules as well as the right to regulate States in this field. In addition, it should be recalled that the use of and access to certain data deemed strategic must be regulated."
10. SGDSN, *Revue stratégique de cyberdéfense* [Strategic Review of Cyber Defense], February 2018, pp. 39-40.

The Villani report recalls that the starting point for any artificial intelligence (AI) strategy involves the creation of large corpuses of data. State authorities should encourage economic players to share and pool data, or even to impose openness in some cases. It should develop and conduct a data policy capable of "being articulated with a goal of sovereignty and capitalizing on European protection standards to make France and Europe the champions of an ethical and sustainable AI".[11] This recent doctrinal production reflects a tension – which is not new but amplified – within state institutions between the proponents of openness of date to fuel economic activity and proponents of transversal protection of data to guarantee digital sovereignty, an essential condition of national sovereignty.[12] The French president resolutely pronounced himself in favor of data openness, through the creation of large public databases.[13]

To the extent that the GDPR relates exclusively to "personal data", the debate raised by its implementation bears mainly on the nature of relations between European consumers and large digital platforms to the detriment of a reflection on "sovereign data", indispensable to the security of governments that have not renounced their jurisdiction or their capacity to assess, decide and act in the international field. This debate tacitly establishes a dichotomy between "personal data" and "sovereign data", even though the former "are no longer granular but reticular, that is, organized in networks". Dynamic, these networks of "personal data" become "continuous flows of information captured and quantified at each moment, linking in real time the data from multiple individual sources",[14] which inevitably leads to questioning their legal nature, and especially their geopolitical and geoeconomic value.

This dimension is curiously neglected even though the data is now presented "as an essential infrastructure for the operation of the economy and the State".[15] In parallel, it has also become an issue of rivalry between nations. Geopolitically, the location of data – primarily that of data centers – constitutes an essential component of any reflection on the subject. Protection of data related to national defense and security involves, for a country such as France, cyber defense provisions aimed at "better

11. C. Villani, *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne* [Giving Meaning to Artificial Intelligence: For a National and European Strategy], Report to the Prime Minister, March 2018, p.25.
12. G. Germain and P. Massart, "Souveraineté numérique" [Digital Sovereignty], *Études*, No. 4242, October 2017.
13. "Emmanuel Macron Talks to Wired about France's AI Strategy", *Wired*, March 31, 2018, available at: www.wired.com.
14. P. Bellanger, "Les données personnelles : une question de souveraineté" [Personal Data: A Question of Sovereignty], *Le Débat*, No. 183, 2015, pp. 17-18.
15. Chief Data Officer, "La donnée comme infrastructure essentielle" [Data as an Essential Infrastructure], Report to the Prime Minister on Data in Government Bodies 2016-2017, French documentation, April 2018.

enforcement of its digital sovereignty".[16] Offensive and retaliatory provisions must also be thought out. Geoeconomically, the location of data refers to the issue of the dominant position exercised by digital platforms, which capture an increasing share of the value produced by the European economy without proportionate returns. On this subject, the EU countries occupy a singular position between the United States and China at a decisive moment, "that of networks that become states that are still slow to become networks".[17] In other words, do the GDPR, the size of the European market and taxation suffice to strengthen its geopolitical and geoeconomic positions? Part of the answer, and only a part, depends on its capacity to develop and conduct a data policy capable of articulating sovereign requirements to European standards and to change the behavior of other players – both governments and platforms – in its favor.

This study focuses on the location of data as an essential but non-exclusive component of a data policy. To do this, it proposes a mapping of the main national measures on this subject (United States, China, Russia, India and Brazil). It then examines the EU's responses by highlighting the geopolitical and geoeconomic issues which should be legitimately taken into account. In other words, data should not only be understood as a commercial and regulatory subject, but as a key element of the digital positioning of its members.

Before going further, let us try to define data both theoretically, officially and then operationally. Theoretically, data remains little thought of, often being compared to oil: it is a raw material in the digital economy. However, "data is both much more complicated and, in the economy it is both much less and much more than oil"; there are fewer rare resources than traces of the real, the number of which is growing exponentially.[18] Officially, the Chief Data Officer defines it as being "the elementary description of numerical nature, represented in coded form, of a reality (thing, event, measurement, transaction, etc.)".[19] Operationally, a start-up owner defines data as "information stored somewhere".[20]

It is this "somewhere" that lies at the origin of this study. In some respects, the question of where the data is located may appear secondary to that of the location of its administrator or the department it is

16. SGDSN, *Revue stratégique de cyberdéfense* [Strategic Review of Cyber Defense], op. cit., p.7.
17. P. Bellanger, "Les données personnelles : une question de souveraineté" [Personal Data: A Question of Sovereignty], art. cit.
18. H. Verdier, "Non, les données ne sont pas du pétrole…" [No, data is not oil…], *Henri Verdier blog*, March 19, 2013, available at: www.henriverdier.com.
19. Chief Data Officer, *op. cit.*, p. 67. Note also that the definition of "reference data", the quality and availability of which are critical for many private and public players such as, for example, the State's geographical reference data, as well as the definition of "pivot data" able to link multiple datasets such as, for example, a company's SIRET number.
20. Interview, December 2017.

associated with, as pointed out by the security director of a software firm.[21] The fact remains that the "entry by geography has the merit of offering a first framework for analysis and being understood by the political decision-maker, still too often disoriented by the technological question, as noted by a designer of cybersecurity solutions.[22]

21. Interview, January 2018.
22. Interview, October 2017.

Mapping and National Positions

Mapping

The problem of the physical location of data is of increasing significance under the twin effect of, on the one hand, development of outsourcing its management by companies or government authorities and, on the other hand, the divergence of legal guarantees governing the protection of personal data between states. With the explosion of global data production (the size of the digital world is expected to multiply by 20 between 2015 and 2025, to reach between 160 and 180 zettabits)[23] and its circulation (the volume of cross-border exchanges of data multiplied by 45 between 2005 and 2014), internal management and data hosting within companies have become increasing resource consumers, particularly of energy and space.[24]

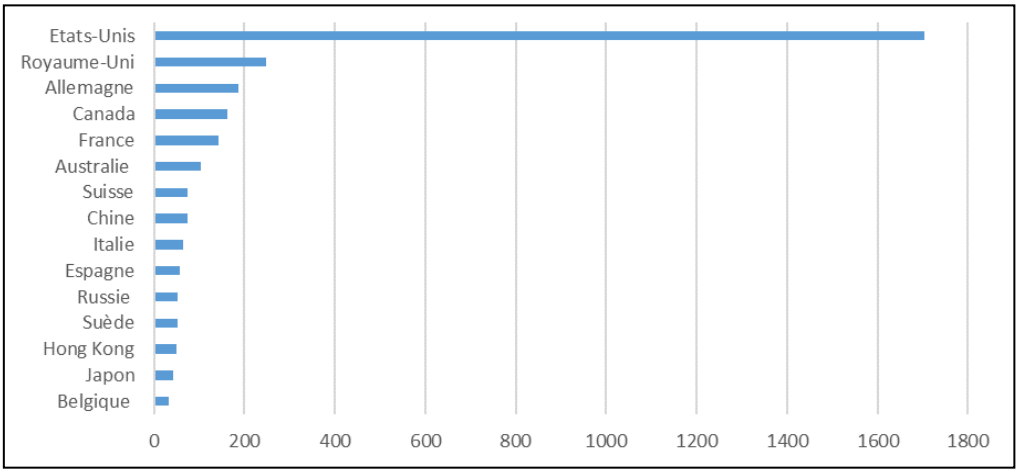
Faced with these difficulties, the expansion of colocation systems and cloud computing[25] managed by the major hosting companies, initially American (Amazon Web Service, Microsoft Azure, Google Cloud, IBM Cloud), has made it possible to achieve economies of scale and take advantage of the network effects inherent in the internet's construction. The share of data stored by these dedicated companies, following this double movement of mass production and the boom in cloud computing, has therefore increased from less than 30% of global data in 2010 to over 50% by 2025, to the detriment of traditional media such as computer hard discs, mobile devices or DVD/Blu-Ray discs.[26] To cope with this exponential increase in the demand for external storage capacity, "*big data centers*" whose processing capacities are constantly increasing, represent in 2018 more than two-thirds of facilities in terms of space occupied, and 44.6% of the building of new data centers.[27]

The trend towards concentration of the sector and the huge size of facilities is intensified globally by the traditional polarization of large

23. D. Reinsel, J. Gantz and J. Rydning, "Data Age 2025: The Evolution of Data to Life-Critical. Don't Focus on Big Data; Focus on the Data That's Big", IDC, April 2017, p. 7.
24. McKinsey Global Institute, "Digital Globalization: The New Era of Global Flows", 2016, pp. 30-37.
25. *Cloud computing* consists of using the calculation or storage power of remote computer servers via the internet.
26. D. Reinsel, J. Gantz and J. Rydning, "Data Age 2025: The Evolution of Data to Life-Critical", *op. cit.*, p. 9.
27. IDC, "Worldwide Datacenter Census and Construction 2014-2018 Forecast: Aging Enterprise Datacenters and the Accelerating Service Provider Buildout", 2014.

colocation sites in the United States, which groups nearly 40% of the world's largest data centers.[28]

Number of data centers per country (2017)

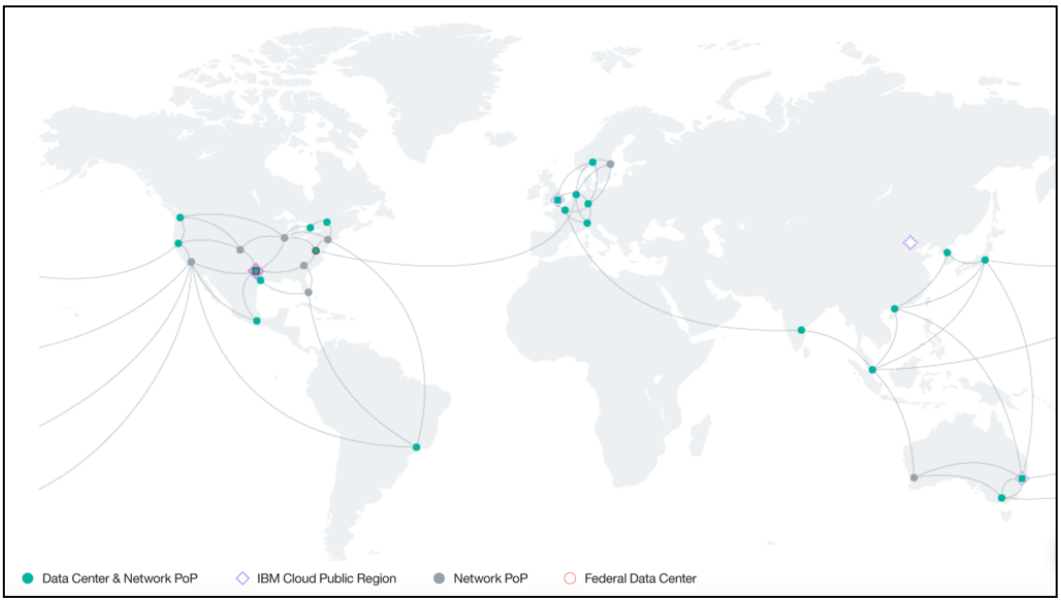


Source: www.datacentermap.com.

The location of data would therefore increasingly echo an "archipelago economy",[29] with a double concentration of facilities in developed countries (in particular the United States) and, within them, at well-connected metropolises hosting the head offices of the largest companies.[30] In Europe, for example, the "FLAPs" (Frankfurt, London, Amsterdam and Paris) are the main interconnection points of telecommunication networks in Europe due to their status as major stock exchange locations[31] and are therefore the main areas for location of European data centers. Added to this model of traditional gravity is a phenomenon of littoralization, consisting of installing numerous data centers at the ends of the world's major submarine cable routes, allowing the development of real continental "gateways" that serve several of the world's strategic regions – in the case of Europe, London for America, Stockholm for Russia and Marseille for North Africa, the Middle East and Asia.[32]

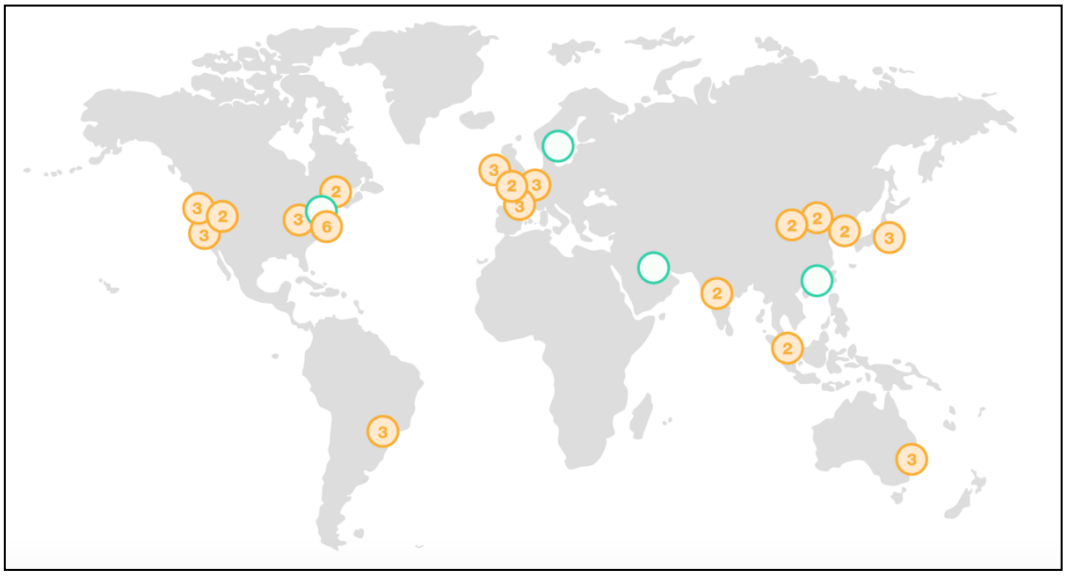
28. See: www.datacentermap.com.
29. To use the expression of Pierre Veltz in *Mondialisation, villes et territoires [Globalization, cities and territories]*, Paris: PUF, 1996.
30. 2,600 data centers out of 7,500 are located in the 20 largest metropolises, according to the *Ovum Global Data Center Analyzer* 2015.
31. Also, the reduction in latency time between storage and processing of data is an essential technical element in "high frequency" trading.
32. As already mentioned, several other factors motive the installation of data centers: price and availability of energy, political and climatic situation, available land, legislative framework, etc. For an in-depth review of these factors, see H. Bakis, "Les facteurs de localisation d'un nouveau type d'établissements tertiaires : les datacentres" [Factors for Location of a New Type of Tertiary Establishment: Datacenters], *NETCOM*, Vol. 27, October 2013, pp. 351-384.

Location of IBM data centers in 2017



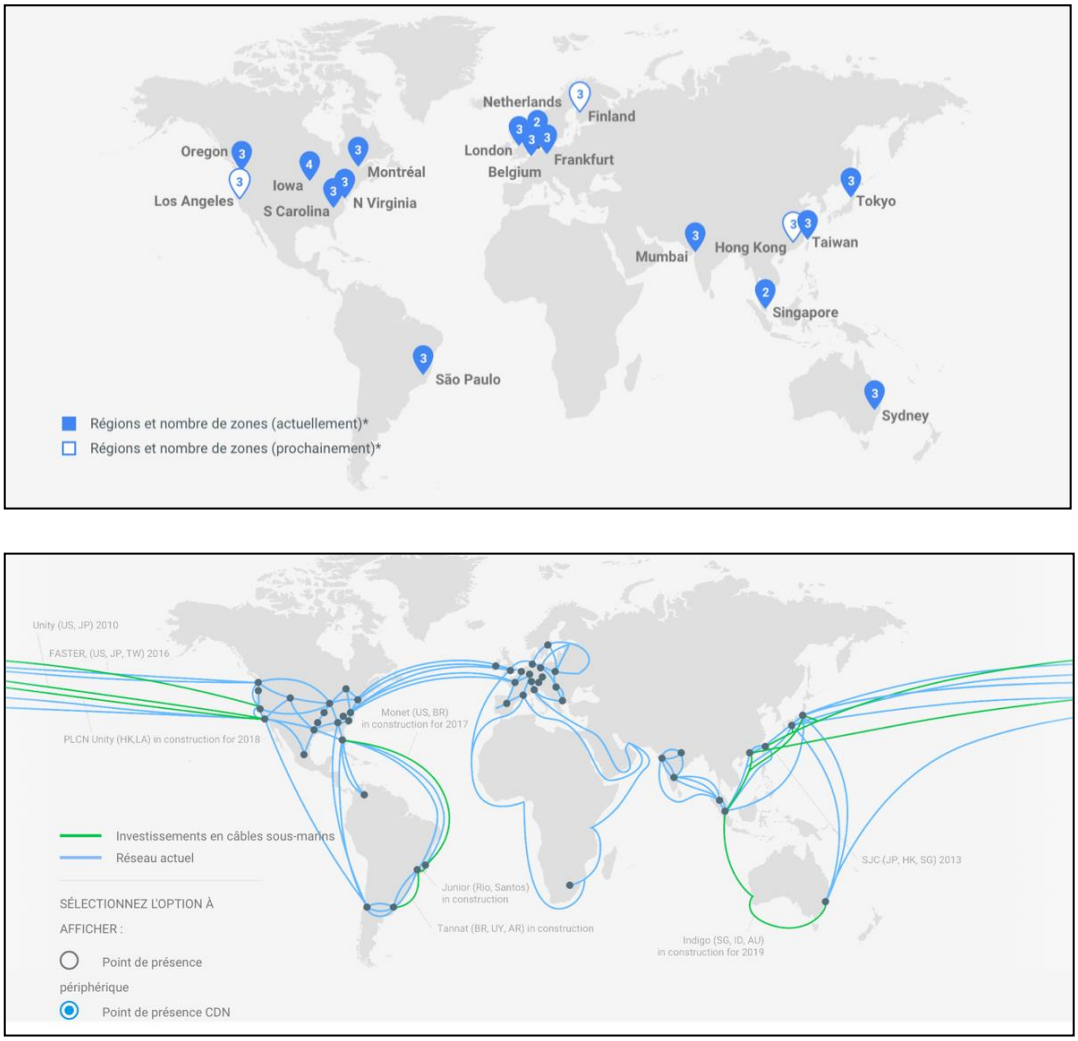
Source: www.ibm.com.

Location of Amazon data centers in 2017



Source: https://aws.amazon.com.

Location of Google Cloud data centers and submarine cables in 2017



Source: www.google.com.

This geography of the location of global data corresponds to the salient and well documented traits of globalization: "triadic" concentration and polarization in metropolises, littoralization via "gateways" of major economic blocs, quantitative and qualitative domination of the United States,[33] catch-up effort by Europeans and major emerging countries.

Nonetheless, several phenomena have challenged this global system based on the free flow of data and its massive processing by American companies on infrastructures located in the United States, calling for a global movement towards reshoring of data. The revelations of Edward

33. For example, until recently the main data centers in Europe were found in countries perceived as having legislation close or very favorable to the major American players: Great Britain, the Netherlands, Sweden...

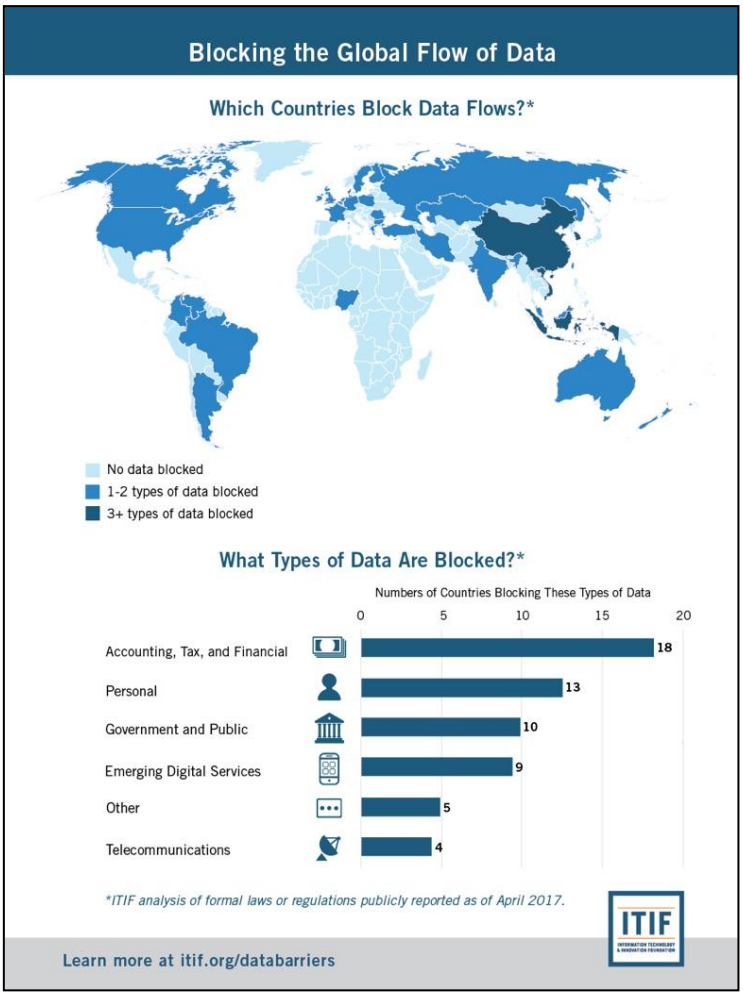
Snowden in 2013 have in this sense been the beginning of a fragmentation – a "balkanization" – of the internet and a politicization of the location of personal data, which has become an issue of national sovereignty and competition between the powers.[34] The transatlantic relationship regarding the transfer and management of personal data has been affected, but other countries such as Russia and China have also become aware of their vulnerability and dependence (see below).

The aspiration to so-called "digital sovereignty" – although this term remains difficult to define in that the state is only one player among others in a largely cross-border digital world[35] – or "digital nationalism"[36] is often translated by measures to impose national preference for the location of certain types of data ("data residency"). Nonetheless, hosting of data on the national territory is now challenged as the most effective way to maintain control and would lead to significant economic costs for countries engaged in such practices, amounting to 0.8% of their GDP.[37]

Government policies to maintain control over data produced by their citizens have therefore taken several forms: support for development of national players and a sovereign *cloud*, limiting foreign investment in the data hosting sector, regulatory limits to the circulation of certain types of data, mandatory duplication of data on nationals on the national territory,[38] "digital pact" for mutual protection, etc.

34. D. Polatin-Reuben and J. Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet", paper delivered at the 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, July 7, 2014, available at: www.usenix.org.
35. For a brief deconstruction of the concept, see J.-P. Derosier, "Les limites du concept de souveraineté numérique" [The Limits of the Concept of Digital Sovereignty], Blog *The Constitution decoded*, October 7, 2016, available at: http://constitutiondecodee.blog.lemonde.fr.
36. C. Kuner, "Data Nationalism and Its Discontents", *Emory Law Journal*, Vol. 64, 2015.
37. United Nations Conference on Trade & Development (UNCTAD), *Data Protection Regulations and International Data Flows: Implications for Trade and Developments 2016*, available at: http://unctad.org.
38. This is the case in Vietnam, for example, since "Decree 72" was published on July 15, 2013, by Prime Minister Nguyen Tan Dung.

What types of data are subject to restrictions?



Source: itif.org.

The dogma of free flow of data, which dominated the expansion of the internet and the digital sphere from the beginning of the 1990s, was therefore severely shaken beginning in 2013. It is now the object of mistrust and questioning for reasons of protection of public freedoms or national sovereignty. From a political point of view, its aggressive promotion by the United States and its allies opposed to the territorialization of data (Australia, Japan and Thailand for the Asia-Pacific Region) is increasingly perceived as a strategy of influence and defending the interest of Anglo-Saxon firms.[39]

39. A report from the Inspectorate General of Finance in April 2016 analyzes the US strategy in detail of promoting the "free flow of data" in multilateral and bilateral trade agreements, as well as its implications for France and the European Union. See P. M. Duhamel *et al.*, "Accord plurilatéral sur le commerce des services et partenariat transatlantique pour le commerce et l'investissement : enjeu numérique des négociations" [Multilateral Agreement on Trade in Services and Transatlantic Partnership for Trade and Investment: A Digital Issue in Negotiations], IGF and General Council on Industry, Energy and Technologies, April 2016, available at: www.economie.gouv.fr.

Debates on these issues on the margins of negotiation of the major trade agreements (RCEP, TiSA, TTIP), which set up the partisans of a data non-localization clause such as those appearing, for example, in Section 14.13 of the TPP,[40] in opposition to States maintaining their right to regulate in this area, thereby constituted the clearest manifestation of the political divisions with respect to an essential and even structural component of 21st century's globalization.[41]

United States

Interactions with the "GAFAM" and self-regulation

No country other than the United States has closely integrated data collection central to its economic and security strategy. The country has a digital industry whose capacity for innovation, power of attraction, market capitalization and economic ambitions far exceed those of other traditional industries. Through the hundreds of billions of data points produced, extracted, "refined", transported and consumed in the world, these platforms create a new form of power of which it is still difficult to outline the contours and implications. Globally, and in support of its industry, the US government promotes "free flow of data", which marks a recent development of American Internet diplomacy, centered for several decades on the free flow of information.

In terms of personal data protection, the differences in approach between the United States and the EU have become considerable, fueling a transatlantic "data war" that took shape in the wake of the Snowden affair.[42]

One of the biggest differences between the European approach and the American approach relates to the commercial or non-commercial character of personal data. In the United States, certain data – for example, data collected by hospitals or banks – have a high level of protection. However, outside these protected areas, companies are free to use data provided they do not commit an "unfair practice". In Europe, personal data are linked to a fundamental right: any use of data is a potential violation of a fundamental right, and must be justified by a legitimate interest, consent, execution of a contract, etc. The American data protection model therefore favors self-regulation and is composed of multiple law, each concerning

40. Section 14.13 of the TPP provides that "a Party shall not require a person to use or locate computer facilities on its territory as a condition of exercising commercial activities on that territory", except "with a view to achieving a legitimate public policy objective".
41. J. Manyika, S. Lund, J. Bughin, *et al.*, "Digital Globalization: The New Era of Global Flows", McKinsey Global Institute, February 2016, available at: www.mckinsey.com.
42. H. Farrell and A. Newman, "The Transatlantic Data War", *op. cit.*

only certain sectors, resulting in unequal protection that is often weaker than in Europe in particular.

On the domestic scene, advances in consumer protection recorded at the end of the Obama presidency was weakened by adoption of an order by Donald Trump compromising the agreement concluded between the United States and the EU and supposedly guaranteeing protection of the data European citizens hosted in American territory. The provisions of the text exclude non-Americans and non-permanent residences from the scope of the law which governs the use of personal data by federal agencies. This leads to questioning the fate of *Privacy Shield*, the Europe-United States framework agreement on the transfer of personal data from Europe, which came into force in the summer of 2017.[43]

Two case studies

Apple/FBI

In 2015, following the San Bernardino massacre in California, the conflict that has long put Apple in opposition to the US government, through the FBI, became the symbol of a political battle of sovereignty between States – which cannot access certain data when investigating evidence of terrorism – and the large digital platforms, which have begun to offer advanced cryptographic tools after the Edward Snowden's revelations about the NSA's mass surveillance.[44]

By refusing to give in to the US government's injunctions to deliver the encryption keys to its iPhone, Apple came to corroborate the unprecedented power of major Internet platforms. Since this controversy, Apple has not renounced encryption of its phones; all the data are encrypted by default and the secret code for decryption is known to each user only, which ensures that Apple cannot communicate this information to intelligence services, if not available.

This case allowed Apple to establish itself as custodian of personal data through its technical device.[45] It has finally come to confirm the centrality of the issue of encryption, crystallizing the point of tension between the higher interest of governments and the requirements of users in respect of privacy.

43. L. Stieglitz, "Quel avenir pour le *Privacy Shield* sous Donald Trump ?" *[What future for Privacy Shield under Donald Trump?]*, Université Aix-Marseille, IREDIC, March 4, 2017, available at: www.iredic.fr.
44. H. Farrell, "Called Out: The Global Consequences of Apple's Fight with the FBI", *Foreign Affairs*, March 7, 2016.
45. A. Joux, "Le conflit des souverainetés : Apple et le FBI" [The Conflict of Sovereignties: Apple and the FBI], *La Revue européenne des médias et du numérique*, No. 38-39, Spring-Summer 2016.

Microsoft Ireland/United States

The leading software publisher refused to deliver emails from an alleged drug dealer required directly by the US court. However, according to Microsoft, the FBI should have gone through international judicial cooperation to obtain emails hosted on its servers in Ireland. In 2016, Microsoft was successful in a US court of appeal, upsetting the Department of Justice. This decision is now in the sights of the Trump administration. A reversal of the US court, through a decision by the Supreme Court, would give it an unprecedented extra-territorial right in digital matters.[46]

For Microsoft, the issue is substantial, due to the successive effect of the *Patriot Act* and the Snowden affair on the confidence of its customers. In response to these challenges, the publisher has invested heavily in construction of data centers located in places chosen for both performance (proximity between the user and the storage location) and for legal issues related to data protection. Since 2013, Microsoft has created data centers in Germany, France, Ireland, the Netherlands and the United Kingdom, and has decided to store the data of Europeans in Europe so it is protected by European rules.

From the point of view of inter-state relations, the fact that governments circumvent international cooperation mechanisms in order to "dig into" data stored in other countries may lead to very strong diplomatic tensions and deeply destabilize international law.[47]

China

Edward Snowden's revelations have only increased the Chinese authorities' efforts to develop a legislative arsenal on cybersecurity and protection of personal data. Like the United States, and unlike Europe and many countries, China has a sectoral approach for data protection: instead of having a major law covering all aspects of personal data protection (like the GDPR), provisions on the subject are disseminated in several texts.

The Cybersecurity Act (2017)

Between protection/data localization…

The law on cybersecurity, which came into force in June 2017, is however part of an evolution towards a more global approach to personal data protection in China. This law specifies the rules that apply to protection of

46. T. Christakis, "La protection de nos données personnelles pourrait être contournée par des pays étrangers" [Protection of Our Personal Data Could Be Circumvented by Foreign Countries], *Le Monde*, January 16, 2018, available at: www.lemonde.fr.
47. American legislation already prohibits internet service providers from giving access to other states to content data (users' emails, etc.) stored on their territory…

personal data and the associated penalties, and defines the rules for international data transfers. For the first time in China, a law regulates the way internet companies can collect, use and store their users' data.

The law's most feared provisions are those requiring certain online services to store their users' data on Chinese territory. The companies concerned are those the text designates as "critical information infrastructures", such as, for example, "communications, energy, transport, water, finance services, public service, e-government and others". This extensive definition can potentially affect all companies, depending on the interest of the Chinese authorities.

Companies are concerned about having to store their data in China, which may require reorganization and substantial expense, while favoring their Chinese competitors. Shadowy areas of the text and its vague wording also make foreign companies worried that they are primarily targeted by the law and be subject to arbitrary inspections, the extent of which is unknown.[48]

… and increased surveillance

This law therefore represents a way for Beijing to protect its data – reflecting a concern about cybersecurity risks in the country – as well as to monitor it. The initiative of the authorities is coupled, as in Russia, with legislation aimed at undoing online anonymity and data encryption.

After the announcement, in January 2017, of a plan to "reclaim Chinese sovereignty of the internet", the government required telecommunication companies to close all access to VPNs before February 1, 2018. VPN applications are very popular with the most connected population of the country and companies, especially multinationals and start-ups established in China, who need to access international services, company servers or sites that are blocked in the country (such as Google and Facebook).

In domestic politics, however, the issue of privacy has become sensitive. In January 2018, the authorities reprimanded several national technology groups on their "inadequate" practices of collecting and securing information about their users, following a rare controversy in the country on personal data protection.[49]

48. S. Livingston, "China Set to Expand Data Localization and Security Review Requirements", International Association of Privacy Professionals, April 25, 2017.
49. M. Jing, "China Warns Internet Companies Over Weak Data Protection Policies", *South China Morning Post*, January 12, 2018, available at: www.scmp.com. Targeted were Baidu, electronic payment platform Ant Financial (associated with the national number one e-commerce Alibaba) as well as the popular application Jinri Toutiao, a news article aggregator.

The Apple case

The Apple case is a perfect illustration of Beijing's aspiration to control "its" data and protect its digital market from the contortions of Silicon Valley giants to continue operating in China.

Apple announced the opening of a data center in China in order to comply with the law on cybersecurity. While Amazon, Microsoft and IBM had already partnered with Chinese companies to operate locally, Apple – by far the most profitable American tech giant in China – had much to lose by refusing to submit to Beijing's data policy, since the local market represents 21% of Apple's global sales.[50]

While the iPhone is one of the symbols of emergence of the Chinese middle class, it has also become the emblem of Chinese dependence on Western technology. Even before the Cybersecurity Act was passed, Chinese authorities were pressuring foreign technology companies to relocate their servers onto Chinese soil. In 2014, Apple transferred a portion of the data from its Chinese users previously located abroad to a data center operated by China Telecom. This change came soon after the public channel CCTV had hinted that Apple was geolocating iPhone users. The new arrangement goes further, however: a Chinese partner (Guizhou-Cloud Big Data) is responsible for management of the data center and for relations with the authorities, particularly in case of a request for data access. Apple will not share the encryption keys for the data center with the Chinese authorities, however. In fact, however, Beijing will have easier access to data stored on its territory, especially due to a change in the way Apple manages the encryption keys needed to unlock an iCloud account. Previously stored in the United States, the keys to Chinese accounts have, since February 2018, been stored in China.

By complying with strict adherence to local rules, Apple maintains thriving sales in China. Unlike Facebook and Google, the Cupertino firm does not sell any product or service with a "political risk" for the Chinese authorities. However, in December 2016 Apple removed new apps created by the *New York Times* from its online app store in China, without specifying the reasons for this withdrawal. Since 2010, $17 billion have been paid to developers in Chins since the launch that year of the App Store in this country.

50. China is Apple's second largest market after the United States.

Russia

The three stages of data localization in Russia

Snowden affair: the first convulsions (2013-2015)

The context that arose from the Snowden affair was timely for Russian political leaders. Domestically, they argued that privacy policies adopted by the major platforms (Google, Facebook, etc.) threaten Russia's digital – and therefore national – sovereignty. In the wake of the revelations, parliamentarians then suggested that all servers on which the personal data of Russian citizens are stored should be transferred to Russia. They launched a media campaign with the aim of placing the major digital platforms under Russian jurisdiction – either by requiring them to be accessible in Russia using the .ru extension, or by obliging them to be hosted on Russian territory.

Parliamentary debates continued for more than a year until the adoption, in the fall of 2014, of the federal law amending previous texts on processing of personal data within information and telecommunication networks. The law aims to limit the use of foreign servers for the collection, retention, processing and storage of personal data of Russian citizens, and to facilitate the State's monitoring activities via the federal agency Roskomnadzor.

Expected to come into effect on September 1, 2014, the law made controversy within the industry which could not comply with the new provisions in time. The negative reactions by many private Russian and international players forced the Duma to reschedule the effective date. The law came into force on September 1, 2015, with nuances in its scope.

Yarovaya laws: counter-terrorism first (2016)

A legislative package introduced by Duma member Irina Yarovaya on the grounds of strengthening the fight against terrorism, the eponymous laws have a dense digital component. They oblige companies that broadcast content over the internet to store on Russian territory, for a period of one year, data relating to the reception and transmission of calls, text messages, photos, audio and video content; telecom operators will keep them there for three years. At the request of security services, telecom operators will also have to provide information about their users and the services they receive. Social media messaging that use additional systems for encryption of messages (such as WhatsApp and Telegram) will have to provide the FSB with the keys to decrypt the content. To the goal of severely suppressing any praising, support or legitimization of an online extremist and/or terrorist activity is superimposed the authorities' desire to combat

encryption of data, for which the major players of the Russian and international digital economy had greatly strengthened standards in the wake of Edward Snowden's revelations.

The Yarovaya laws immediately aroused strong criticism among private operators. Burdening the mobile operators and the digital industry with the cost of storing metadata, by construction of data centers on Russian soil, the authorities are jeopardizing the future of this industry in Russia while sending a negative signal to foreign investors. Yandex and Megafon also expressed their concerns about the financial cost of complying with the new provisions and its technical feasibility.

Since 2017: breaking data encryption

From a security angle, all the provisions on relocation of data may be interpreted by the willingness of the Russian authorities to combat the https protocol, especially used by Gmail, Facebook, Twitter and Wikipedia. Russian internet surveillance systems cannot "handle" the https protocol because of the encryption standards used. Ahead of the March 2018 presidential election, the authorities tackled the tools and platforms enabling circumvention of surveillance and censorship.

So two laws were enacted in the summer of 2017. They prohibited the use of software to circumvent website blocking (VPNs or proxies or the TOR network – used more and more by Russian internet users), censor the search engines and control instant messaging apps. Practically speaking, suppliers of such software must now cooperate with the authorities for blocking of sites in Russia. The law requires search engines to remove any reference to sites blocked in Russia. The other legislation targets instant and encrypted messaging such as WhatsApp and Telegram. These two operators must now cooperate with Russian mobile operators for identifying their users and block messages at the authorities' request.

Differentiated responses

Enactment of these laws has provoked many reactions in Russia, with national and foreign private players responding differently according to their interests.

Blocking of LinkedIn

In November 2016, the Russian courts ordered the blocking of the LinkedIn professional social media on the grounds of non-conformity with the Russian law on personal data. For the first time, a Russian judge ordered the registration of a foreign website of such large scale in the register of perpetrators of infringement of the law on personal data.

After the judgment, LinkedIn did not undertake any action to locate its databases in Russia, and access to its site was therefore blocked shortly after. For some, this judgment signaled the end of the transition period during which Roskomnadzor was tolerant of setting up data storage platforms in Russia even though the localization requirement was already in force. For others, it is a test to study the reactions of the population before a potential closure of other foreign social media.[51] The LinkedIn decision may be explained by economic considerations: like many other global websites, LinkedIn does not have a separate server for users in every country in the world, due to the high cost this would represent.

Telegram's maneuvers

Roskomnadzor's threats to block the Telegram encrypted messaging service in Russia began in a media battle between app cofounder Pavel Durov and federal agency head Alexandre Jarov. The entrepreneur – already cofounder of VKontakte before being forced to sell his shares and exile himself from Russia in 2013 – persisted in his refusal to comply with the provisions of a 2014 law requiring "information distributors" to register in Russia, store all connection data of their users for six months and make it available to the authorities on request. Durov finally agreed to register, while insisting that we will not share the data of Telegram users nor Telegram's encryption keys.

Facebook and Twitter comply

After two years of delay and negotiations with the Russian authorities, Facebook and Twitter announced in November 2017 their compliance with Russian legislation on data location. Twitter in particular announced it would relocate its Russian users' data to servers in Russia by mid-year 2018. Facebook agreed to submit to Roskomnadzor without communicating its strategy, merely announcing the opening of a representative office in Moscow.

The pressure on these two platforms coincided with US congressional investigations into suspicions of targeted advertising by Russia on these social media in order to influence the outcome of the presidential election.

Between strict application of the law and political decision, the boundary remains tenuous, in the case of the Russian authorities, with regard to data policy. Two factors of political nature cannot be understated: internally – the Kremlin will seek to protect itself from the potential for mobilization enabled by Internet platforms – and externally – the particularly tense context of the Russian-American relationship. These two

51. "Mosgorsud razrešil zablokirovat' LinkedIn v Rossii", blog of Ilya Varlamov, November 10, 2016, available at: https://varlamov.ru.

dimensions combine in an ambition of technological self-sufficiency, retaining all proportions, similar to that of China.

India

Inaugurating "Digital India Week" in July 2015, Prime Minister Narendra Modi affirmed India's vocation to become a "digital power" and to play a role in the rivalries surrounding the circulation and location of global data.[52]

Less than three years later, India's digital policy is at a major turning point. A succession of controversies – security vulnerabilities striking the world's largest biometric database "Aadhaar",[53] failure of the "Digital India" flagship program – has led the government to set up a committee of experts led by Judge B. N. Srikrishna to build an overall architecture of security and protection of personal data in India.

Indeed, by the first quarter of 2018 India does not yet have a comprehensive regulatory framework dealing with data location, circulation and privacy protection, while the country already has close to 450 million internet users.[54] A report by the Shah committee, published in 2012, should have resulted in such a regime, but it was never followed up. This persistent gap in protection of users has increasingly resonated since early 2018 with the backlash from the Cambridge Analytica affair in India[55] or the revelation by a French computer scientist of the unauthorized processing of the data of 5 million users of Prime Minister Modi's application.[56] Political and legal[57] pressure to put an end to the world's largest "Wild West of data"[58] with a robust and protective legal system is at its highest. It is in this context that the Srikrishna committee submitted its report at the end of May 2018, as well as a draft bill relating to protection of personal data.[59]

Discussions within this high-level committee, as reflected in the White Paper on Data Protection published in November 2017, are fully informed by European and American models of legislation, whose advantages and

52. Opening speech by Narendra Modi at the Digital India Week, July 1, 2015, available at: www.youtube.com.
53. S. Farcis, "Inde : une journaliste prouve la vulnérabilité d'Aadhaar, énorme base de données" [India: A Journalist Proves the Vulnerability of Aadhaar, a Huge Database], RFI, January 11, 2018, available at: www.rfi.fr.
54. Internet and Mobile Association of India and IMRB, "Internet in India – 2016", February 2017, available at: http://bestmediainfo.com.
55. G. Delacroix, "Le scandale Facebook s'étend en Inde" [The Facebook Scandal Extends to India], *Courrier international*, March 23, 2018, available at: www.courrierinternational.com.
56. E. Derville, "Émoi en Inde sur la protection des données" [Emotion in India on Data Protection], *Le Figaro*, March 28, 2018, available at: www.lefigaro.fr.
57. Appeals relating to personal data before India's Supreme Court have considerably increased as a result of the Adhaar scandal.
58. D. Boullier, *Sociologie du numérique*, Paris: Armand Colin, 2016.
59. J. Gandhi, "Srikrishna Committee Report on Data Protection and Privacy by May-end", *Hindustan Times*, March 27, 2018, www.hindustantimes.com.

disadvantages are carefully weighed.[60] The global trend toward "sovereignization" of the Internet since 2013 is also identified, and in this context committee members believe that India should position itself at a moderate level compared to existing levels of restriction, both to preserve the attractiveness of its territory and to support development of its technology enterprises. In addition, the right to privacy has recently been recognized by the country's Supreme Court as a fundamental right protected by the Constitution in a *Puttaswamy* order (2017), leading to a more liberal interpretation of the data issue by the authorities, a question which, moreover, is addressed as a priority from the standpoint of protection of rights by the Srikrishna committee.

The law in force, based in particular on rules published by the Ministry of Telecommunications and Technology in 2011, is in fact more restrictive than European and American laws on location and circulation of data. For example, Indian companies that collect data in India must obtain the explicit consent of their users before being able to transfer their data abroad or demonstrate the "necessity" of this transfer.[61]

In terms of national security, India has developed several instruments that impose data localization on foreign companies: following the attacks in Bombay in 2008, New Delhi forced several encrypted messaging service operators such as Research In Motion (BlackBerry) and Nokia to keep their data on national territory to respond to the requests of intelligence agencies.[62] In 2014, as a direct result of the Snowden leaks, the National Security Council even proposed that all data concerning Indian citizens be mandatorily stored on the national territory and subject to local law. Faced with the opposition of the digital industry, the project was abandoned.

Certain types of data are also subject to increased precautions due to their sensitive nature. For example, a law of 1993 prohibits the transfer abroad of data of government origin, except for objectives pursued by the government itself.[63] This regulation was extended in 2012 to data collected using public funds by the *National Data Sharing and Accessibility Policy*[64] and since 2015 public contracts for cloud computing have contained a territorialization clause. In this perspective of hosting and securing public data, the Indian government has developed a sovereign cloud, the MeghRaj Cloud, consisting of a network of data centers that are both public and

60. Indian Ministry of Electronics and Information Technology, "White Paper on Data Protection Framework for India", available at: http://meity.gov.in.
61. A. Chandler and P. Lê Uyeˆn, "Data Nationalism", *EMORY Law Journal*, Vol. 64, 2015, pp. 678-682.
62. "Big Brother Must Not Overstep the Limits", *Tehelka*, March 3, 2012, available at: www.tehelka.com.
63. Section 4 of the Public Records Act, 1993.
64. N. Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", Information Technology & Innovation Foundation, May 1, 2017, available at: https://itif.org.

private and located throughout the country. Facilities owned by private service providers within the MaghRaj network are subject to increased security standards and regular audits. Finally, financial data are also affected by specific provisions: the *Companies (Accounts) Rules Law* of 2014 requires Indian companies to keep on servers located in India a copy of their sensitive financial data, if they are stored abroad.

Nevertheless, the approach by the Indian authorities regarding location and protection of data is strongly influenced by economic considerations and the willingness to support the growth of a local ecosystem of data hosting companies (Netmagick, Reliance, Tata Communications, CtrlS…).[65] In the context of reflections about the new legislation on personal data, groups of technology companies have defended the free flow of data as a *sine qua non* condition of the sector's development in India.

The Srikrishna committee has echoed these economic concerns.[66] In this perspective of attractiveness and development, India would like to demonstrate that foreign data stored on its territory benefits from important protections: the "digital pact" signed in 2012 between India and the United Kingdom on protection of British data stored in India is a strong diplomatic initiative in this direction. More broadly, it appears that the data management model in India is moving towards a more liberal design than previously, influenced by the interests of a strong private sector and by the GDPR model of data protection.[67] It nonetheless appears that the authorities are retaining a margin for maneuver in the definition of sensitive data, the extent of which is expected to evolve in relation to the 2011 text and to the degree of territorialization to which they will be imposed. The search for an "à la carte" approach suited to Indian realities is therefore at the heart of the initial work of the Srikrishna committee:

> "The study of all these practices shows that several countries have put data location policies in place in one way or another. However, most countries do not deem it relevant. India will have to carefully weigh the costs and benefits of such provisions. Different types of data should be treated differently, depending on their importance to the economy and the population. It seems that a single model for all data ("one

65. India is the second largest data center market in the Asia-Pacific region with 5.23% of the area's facilities in 2015 and the fastest growth after China. See on this subject: Internet and Mobile Association of India (IAMAI), "Make in India: Conducive Policy and Regulatory Environment to Incentivize Data Center Infrastructure", May 2016, p. 5, available at: www.iamai.in.
66. B. N. Srikrishna., "White Paper of the Committee of Experts on a Data Protection Framework for India", Committee of Experts of the Indian Government, November 2017, available at: http://meity.gov.in.
67.The weight of the Indian private sector and the support of the "multi-stakeholder" model of governance have made India focus more on the Western approach to data sovereignty than the Sino-Russian model. See D. Polatin-Reuben and J. Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanization of the Internet", *op. cit.*

> size fits all") is not the most appropriate. Therefore, while location of data can be envisaged in certain sensitive sectors, this approach should not be made general".[68]

While the committee is expected to make public its recent work and a draft regulation on July 15, 2018, recent leaks have revealed divisions among its members on the issue of data location, which could ultimately be imposed on all players in the sector.[69] These hesitations emerged in April 2018 when the Indian central bank required all payment service providers to store their data in India. This shift to a defense of data localization, if confirmed, would be a break with the goal of protecting the interests of the Indian digital industry and the more liberal approach outlined in the November 2017 report.

Brazil

Edward Snowden's disclosures in 2013 have had a particularly strong influence on Brazil's digital policy, of which leader Dilma Rousseff and several executives of the government and the Petrobras State enterprise have been the subject of NSA surveillance.[70] The Brazilian leader reacted in a very firm manner by deciding to change the balance of the digital bill discussed since 2009, the *Marco Civil da Internet*, whose spirit, initially turned to protection of liberties, was more oriented under her impulse towards the problems of digital sovereignty. This shiftin Brazilian data policy was expressed by Dilma Rousseff on September 24, 2013, at the United Nations General Assembly:

> "A sovereign State cannot consolidate to the detriment of others equally sovereign. The right to security of citizens of a country can in no case be guaranteed by the violation of the fundamental rights of citizens of another country. [...]Brazil knows how to protect itself and will redouble its efforts to adapt its laws and technologies for this purpose."[71]

The new version of the *Marco Civil da Internet* included a new article 12 that allows the executive to compel internet providers and digital applications to store and process their data on Brazilian territory. Nonetheless, when the text was adopted in April 2014, this provision was

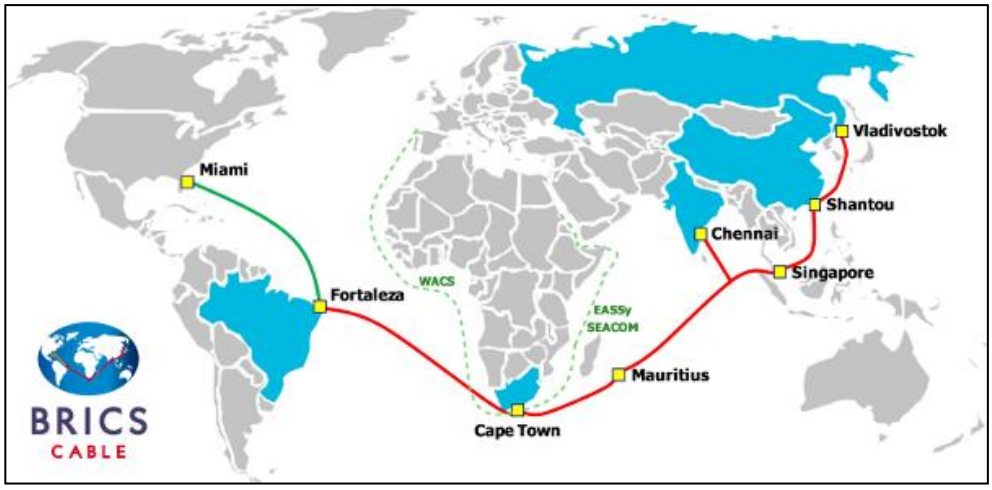
68. B. N. Srikrishna, "White Paper of the Committee of Experts on a Data Protection Framework for India", *op. cit.*, p. 75.
69. "Justice Srikrishna Committee May Ask MNCs to Store Data in India", *Business Today India*, June 18, 2018, available at: www.businesstoday.in.
70. J. Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobras", *The Guardian*, September 9, 2013, available at: www.theguardian.com; B. Winter, "Exclusive: Brazil's Rousseff Wants U.S. Apology for NSA Spying", Reuters, September 4, 2013, available at: www.reuters.com.
71. D. Rousseff, "Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly", September 24, 2013, available at: www.un.org.

deleted and replaced by an extension of the extraterritorial jurisdiction of the Brazilian judge on personal data of Brazilian citizens stored abroad.[72]

Over the 2013-2014 period, Brazil also initiated several diplomatic approaches aimed at reducing its dependence on data flows from the United States, notably via submarine fiber optic cables under the "Tempora"[73] operation. Dilma Rousseff intended to take advantage of the port of Fortaleza as a historic "gateway" for Latin America to circumvent American territory by relaunching the "BRICS cable" project linking Fortaleza-Cape Town-Chennai-Shantou-Vladivostok.[74]

Nonetheless, divergences of interest and the design of internet governance between the BRICS led to failure of the project in 2014[75]: to the Sino-Russian model of digital sovereignty, Brazil, India and South Africa preferred a development of international bodies to a multi-stakeholder governance, materialized during the NETmundial forum organized in São Paulo in April 2014. As a sign of this original and independent positioning, Dilma Rousseff also defended creation of a Brazil-Europe link between Fortaleza and Lisbon, effectively initiated at the 7th Brazil-EU summit on February 23, 2014.

BRICS internet cable project



Source: Infowars.com.

72. D. Cooper, "Brazil Enacts 'Marco Civil' Internet Civil Rights Bill", *Inside Privacy*, April 28, 2014, available at: www.insideprivacy.com.
73. The Tempora operation of the GCHQ allowed the British service to connect directly to transatlantic internet cables to listen to all information flows. See for example E. MacAskill, J. Borger, N. Hopkins, N. Davies and J. Ball, "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications", *The Guardian*, June 21, 2013, available at: www.theguardian.com.
74. P. J. Watson, "BRICS Countries Build New Internet to Avoid NSA Spying", *Infowars.com*, October 24, 2013, available at: www.infowars.com.
75. A. Zyw Melo, "Un câble pour les BRICS : un défi stratégique insurmontable" [A Cable for the BRICS: An Insurmountable Strategic Challenge], *Hermès*, Vol. 79, No. 3, 2017, pp. 145-149.

This desire to place Brazil at the center of alternative data traffic routes to make a Latin American, or even South Atlantic, digital hub is accompanied by an industrial strategy dating from the early 2000s, aiming at attracting global players in data hosting while favoring the emergence of national players.

Google's installation of its first Latin American data center in Chile, in 2012, was seen as a failure by the country's authorities, which was suffering from a domestic cost that was too high for the installation of data centers,[76] a very bad position (which persists today) in the country-risk rankings regarding the location of the data.[77] This willingness has notably resulted in tax benefits and measures favoring local businesses, such as the Totvs company, whose growth has benefited greatly from the support of the Brazilian Development Bank under the Prosoft program.[78] Creation of an alternative to Microsoft Outlook for Brazilian government communications, Expresso V3, operated via a sovereign cloud installed in 2013 by the Federal Data Processing Service, reveals this desire to build autonomous capacities for the purposes of protecting sensitive data.

Brazil is in the process of adopting a comprehensive legislative framework for protection of personal data. Two competing texts are being reviewed, one by the Senate,[79] the other by the Chamber of Deputies.[80] The latter, more recent and largely inspired by the European GDPR, was adopted by the Senate's Economic Affairs Committee on July 3, 2018. This text would replace sectoral regulations (health, banking sector, etc.) while supplementing the *Marco Civil da Internet* and its implementing decree. It is inspired by the European example of comprehensive and protective legislation, adopting for example notions such as "equivalent protection" for data transfer or that of "explicit consent". It also includes the definition of sensitive data contained in article 9 of the GDPR. Nonetheless, the protections offered appear to be less than those of the European regulation and confirm Brazil's median position, which had already emerged at the NETmundial, between the European conception of protection of personal data and the attachment of some form of digital sovereignty for the major emerging countries.[81]

76. L. Chao et P. Trevisani, "Brazil Legislators Bear Down on Internet Bill", *The Wall Street Journal*, November 13, 2013.
77. Brazil is still 32nd out of 37 countries evaluated by Cushman & Wakefield's *Data Center Risk Index 2016*.
78. F. Malerba, S. Mani and P. Adams, "The Rise to Market Leadership: New Leading Firms from Emerging Countries", Northampton: EE Publishing, April 2017, pp. 177-179.
79. Projeto de Lei do Senado No. 330, de 2013.
80. Projeto de Lei da Câmara dos Deputados No. 5276, de 2016.
81. J. Nocetti, "Puissances émergentes et internet : vers une troisième voie ?" [Emerging Powers and the Internet: Towards a Third Way?], *Politique étrangère*, Vol. 79, No. 4, 2014, pp. 50-51.

The European Union's Response

The mapping presented in the first section illustrates the implementation of policies of assumed "digital sovereignty" or "sovereignty in digital space" that are observed on several levels. Control of data often requires a political will to localize them on the national territory through a specific policy towards data centers aimed at protecting and integrating this sector. More broadly, this sovereign approach is observed, again differently depending on the country, in the conception of cyberspace, both in its physical layer (national infrastructure), logic (software and applications) and semantics ("national" content).

The GDPR: alpha or omega?

The GDPR is a regulatory response to a geopolitical challenge launched by the United States to Europe and all of its allies. Due to the international situation, the asymmetry of power relations in the digital world and the mistrust that followed revelations of American mass surveillance, the current trend is the multiplication of data localization measures in national legislative arrangements. The level of economic interests at play explains the outbreak of sometimes virulent debates. From an economic perspective, the free flow of data, coupled with reasoning about the value produced by this flow, is often opposed to a form of digital protectionism that would necessarily lead to a barrier to innovation and financial loss.[82] This free flow of data was at the heart of several draft free trade agreements negotiated by the United States such as the Transpacific Partnership signed with 11 countries of the Asia-Pacific region (TPP) and the Transatlantic region (TTIP) as well as the Trade in Services Agreement (TISA).[83] Conversely, politically and well before Edward Snowden, voices were raised to denounce a risk of "digital imperialism", particularly in Europe.[84] In France, for example, two parliamentary reports (2013 and 2014) converged on this idea by warning on the risks, for the French and European

82. N. Mishra, "Data Localization Laws in a Digital World", *The Public Sphere Journal*, 2016, pp. 135-158.
83 The United States disengaged from the Transpacific Partnership, signed in February 2016, in January 2017. The subject of lively criticism in Europe, both about the negotiation process and the content of the agreement itself, the Transatlantic Partnership has not led to a consensus between Europeans and Americans. The Trade in Services Agreement meanwhile is still being negotiated between some fifty countries, including the United States and the States of the European Union.
84. J. Nocetti, "Puissances émergentes et internet : vers une troisième voie ?", *op. cit.*, p. 55.

economy, of being overwhelmed by the American "military-digital complex". The Snowden affair superimposes on these critics a security dimension on the confidentiality of data and the risks to personal data.

The novelty of the GDPR is based on the establishment of three main principles: a rationale of corporate accountability for protection of personal data, the co-responsibility of subcontractors and the imposition of the notions of "privacy by design" and "privacy by default".[85] This set of rules provides a harmonized framework for the whole of the EU and applies extraterritorially to all enterprises, European or not, every time a European resident is directly targeted by data processing, including over the internet. With the GDPR, the EU becomes one of the world's most stringent data protection systems: for community institutions, it is a matter of clearly posting in law the values that the EU is based on: respect for fundamental rights and certain ethics with respect to individual privacy.[86]

The GDPR may be read as "a rather virulent reaction of Europe" with regard to "the United States which understood that we had the ability to protect our information", according to the representative of the Ministry of the Interior.[87] Implementation of the GDPR comes in a context of a potential transatlantic trade war. It is still too soon to anticipate the reactions of the American authorities to any fines imposed on American platforms. However, they will have to be analyzed not only in terms of litigation, but also on the basis of the different components of the transatlantic relationship. In the event of a crisis, at least three components must be carefully observed: the commercial component with the setting up of tariffs on products such as steel; the security component through NATO and the bilateral relations maintained by Washington with each European capital; the legal component with the possibility of seeing the rationale of *nexus*, extended to the use of the internet or American software.[88] Some artisans of the GDPR do not conceal their perplexity about its real effectiveness, because "we are leaving right to move into balance of power".[89] The whole point is to know if the EU is sufficiently equipped to exercise this balance of power and what will be its level of political determination to do so, since some of its members have close ties with Washington on intelligence matters.

85 General Data Protection Regulation, Official Journal of the European Union, May 25, 2018, available at: https://eur-lex.europa.eu
86. Interview with Isabelle Falque-Pierrotin in *La Tribune*, March 27, 2018.
87. Interview, November 2017.
88. M. Leblanc-Wohrer, "*Comply or Die*? Les entreprises face à l'exigence de conformité venue des États-Unis" *[Companies Face Compliance Requirements from the United States]*, *Potomac Papers*, No. 34, Ifri, March 2018, pp. 17-19, available at: www.ifri.org.
89. Interview, December 2017.

From their side, the large digital platforms have prepared themselves for implementation of the GDPR by following its preparation very closely. Some parliamentarians are openly questioning the means of control available to European authorities.[90] These political concerns are relayed by technical considerations expressed by this French cybersecurity specialist: "Technically, it is impossible to ensure that a company does not collect data or to ensure that data has actually disappeared." According to him, it would ultimately be impossible to verify the reality of commitments made by the platforms on the data of European citizens: "There is a naivety and sense of allying with the United States".[91] Naivety, to the extent that European countries and enterprises are in a fundamentally unfavorable balance of power in the face of the power of the American military-digital complex. Sense, to the extent that this subordination is part of a rationale of alliance and sharing of values affecting public and individual freedoms as opposed to the behavior, in this field, of an authoritarian regime such as China. According to a public affairs official for one of the GAFAM, the GDPR "is great" because it gives clear direction to the platforms; the regulatory aspects are necessary to attempt to "control the technology".[92] The B2C rationale of the GDPR could, in his view, evolve into a B2B rationale and thereby strengthen the value of a global cloud.

Is digital decolonization possible?

The aftermath of the Snowden affair and preparation for the GDPR have led to numerous discussions on the nature of transatlantic relations that are increasingly dependent on management of data flows. In October 2015, the European Court of Justice (ECJ) invalidated the decision by which the European Commission had found that the United States was providing a sufficient level of protection for transferred European personal data. This decision ended the *safe harbor* established in July 2000, which considered that the United States provided a sufficient level of protection of personal data of European citizens transiting through American platforms, which would have been transferred by the American authorities into intelligence instruments.[93]

The positions of the two parties are explained by profoundly different legal conceptions. In Europe, protection of privacy and of personal data is a fundamental right, while in the United States the 4th Amendment to the Constitution guarantees a right to privacy, "but only with respect of the

90. Interview, November 2017.
91. Interview, January 2018.
92. Interview, November 2017.
93. H. Farrell and A. Newman, "The Transatlantic Data War", *op. cit.*, p. 131.

government".[94] In addition, the constitutional right only applies to American citizens and to foreigners who live on American soil, and does not concern privacy infringements committed by private players. From there, one of the big differences between the American and European approaches lies in the commercial character, or not, of the personal data. In the United States, companies can use it as long as they do not commit an "unfair practice". In Europe, any use constitutes a potential violation of a fundamental right. Although the starting point is fundamentally different, the respective approaches often lead to the same practical result.

Based on this observation, several think tanks have replaced the debate on data in the transatlantic framework to strengthening it by accentuating the convergences rather than the divergences. In 2016, the *Atlantic Council* advocated the creation of a transatlantic digital market, which would extend "from Silicon Valley to Tallinn".[95] According to this report, the United States and the EU were facing a "historic opportunity – perhaps the last – to be the leaders" of the digital market, and its recommendations were placed directly in the double framework of negotiations for the *Transatlantic Trade and Investment Partnership* (TTIP) and provided four main measures in view of improving data protection and privacy, including by distinguishing between personal and industrial data.[96] In June 2017, a report by Chatham House found that a global consensus on data regulation was out of reach and therefore proposed the development, as a minimum, of a *Transatlantic Charter for Data Security and Mobility*, establishing mechanisms for cooperation between the two parties.[97] In July 2017, a task force of the *Council on Foreign Relations* met to analyze the causes of "digital protectionism", which would be at work both in Asia and Europe. While clearly distinguishing the Chinese and European policies, the task force severely criticizes the latter, believing that it reflects a rationale of regulation by law while ignoring the interactions between privacy, security and innovation peculiar to the digital economy. The localization of data creates a "regulatory burden" that is unfavorable to American firms and reflects the "Anti-American bias" of the European approach. The task force stresses

94. W. J. Maxwell, "La protection des données à caractère personnel aux États-Unis : convergences et divergences avec l'approche européenne" *[Protection of personal data in the United States: convergences and divergences with the European approach]*, p. 1, available at: www.hoganlovells.com.
95. Atlantic Council, *Building a Transatlantic Digital Marketplace: Twenty Steps Toward 2020*, Report of the Atlantic Council Task Force on Advancing a Transatlantic Digital Agenda, April 2016.
96. *Ibid.*; Play an active role in the revision of the Council of Europe's Convention 108; Expand the discussion on thresholds and legal distinctions for personal data for the era of big data and the Internet of things; Explore discrete sectoral confidence-building measures (CBMs) centered around users' access to their data, user privacy and user security; Integrate cybersecurity more fully into transatlantic discussions on privacy policy.
97. C. Smart, *Regulating the Data that Drive 21st-Century Economic Growth: The Looming Transatlantic Battle*, Research Paper, Chatham House, June 2017.

that these regulatory constraints will affect small and medium companies more than the large platforms originally targeted.[98]

In addition to the satisfaction expressed with respect to the GDPR, they take the following argument to better emphasize their centrality and power compared to the European authorities.[99] First, they point out that they have R&D investment capabilities that are far greater than those which Member States are likely to mobilize. Secondly, they point out, based on the examples of the United States, China and Germany, that with respect to security data, any sovereign cloud has a much higher cost. In this perspective, they propose offers guaranteeing the localization of data within a European country "but with a global administration capacity". This leads a computer security specialist to emphasize the following point: "What is fundamental is not the data center, but the associated service".[100] Thirdly, the large platforms hold a geometrically variable discourse with regard to China. With respect to the Europeans, they point out that it presents more risk in terms of security or respect for intellectual property than the United States. With respect to the Chinese authorities, they are competing for market share, while explaining "that it is important that the West is present in China" by being aware of ethical issues.

Unsurprisingly, cybersecurity specialists believe that digital flows are increasingly being encrypted to guarantee the integrity of the information transmitted. In this context, the strategic challenge lies in control of the encryption keys produced and located in Europe, which involves a double process of trust and standardization because "it must be certain that the data is encrypted according to European standards".[101] According to some direct competitors of the GAFAM, "it is clear that the United States is seeking to get its hands on European certification and approval" and that American platforms and equipment manufacturers want to "register their products as trusted products", recognized as such by the European authorities.[102]

The polymorphic nature of the domination exercised by the American platforms makes digital decolonization efforts random, to the extent that personal data fuels economic competition and management of security data betrays the fundamental ambivalence of Europeans towards the United States. Most members of the EU are allied with the United States in

98. Council on Foreign relations, "The Rise of Digital Protectionism", Insights from a CFR Workshop, October 2017: "One participant summed up Europe's approach to the digital economy as 'not protectionist, just flawed – and wrong'".
99. Interview, November 2017.
100. Interview, January 2018.
101. Interview, October 2017.
102. *Ibid*.

NATO and for the most part, rely exclusively on the Atlantic Alliance to ensure their national security.

The nature of relations with the United States

Designed for protection of personal data, the debate preceding the establishment of the GDPR evaded two fundamental questions. The first concerns its technological and industrial consequences. A computer security specialist expresses an idea widely shared by companies subject to the omnipotence of GAFAMs: "The GDPR is a European legal response that will be useless" without the emergence of European industrial players capable of competing with the GAFAMs.[103] The Villani report undercuts this idea by indicating that it is not necessarily via a "European Google" that France and Europe will be able to make themselves a place on the world stage in AI matters, but in particular by "an offensive policy to promote access to data".[104] This difference of viewpoint arises from noting that the EU has preferred to allocate its political resources to development of a regulatory tool rather than kindling an industrial dynamic, and in doing so consumes resources without provoking the effect of technological acceleration, at the moment. In other words, European countries no longer seem able to launch programs having a major effect, like some of them had been able to do in the nuclear, aeronautics or space domains.

The second question evaded by the debate on the GDPR precisely concerns the articulation between private data and security data. By focusing on personal data, the EU defends, as we have seen, a consumer rights approach. It is all the more paradoxical that the Regulation was presented as the EU's political response to Edward Snowden's revelations on the existence of massive surveillance programs justified by combating terrorism. With Edward Snowden, European opinions have become aware of the degree of American intrusion in information systems. The Europeans are faced with the following contradiction: they benefit, in various contexts, from information provided by their American ally, which exploits both personal data and security data; they submit to American intrusions, which steal security data, as well as the domination exercised by the GAFAM, who exploit their personal data. The Europeans therefore give the impression of being blind with respect to data. The only way to control data security is to locate and exploit them in a strictly national ecosystem:

103. Interview, January 2018.
104. C. Villani, *op. cit.*, p. 25.

"this is the path chosen by the United States, China and Russia, but not by Europe due to its neo-liberal ideology".[105]

Regarding the partnerships that France should establish in respect of exchanges of security data or their protection, interviews conducted reflect a debate underlying France's security policy on the balances to be found between its nearest allies: the United Kingdom, Germany and the United States. After Brexit, the election of Donald Trump, that of Emmanuel Macron and Angela Merkel, the relations by Paris with London, Berlin and Washington are in the process of change.[106] Not widely publicized, discussions on digital issues and, in particular, on data exchanges are an indicator of alliance.

The *Strategic Review of Cyber Defense* notes the differences in model between the four allies. The French model of cyber defense is based on the separation of offensive and defensive capabilities, while American capacities are largely concentrated within the intelligence community. By pooling national technical skills within the NSA, the American model poses "the problem of acceptability by the private sector of State intervention in security of information systems".[107] The British model is closer to the American model, while the German model "translates a vision of cyberspace very close to that of France"; "This proximity makes Germany a privileged partner of France within the various international fora dealing with these subjects and gives the French-German pair a role of major impetus in European projects relating to information system security".[108]

Earlier, the *Strategic Review of Defense and National Security* had presented Germany as "a key partner in strengthening a European defense and security ambition" and had recalled that "the United Kingdom and Germany are strategic intelligence partners".[109] With Brexit, there will no longer be countries belonging to the *Five Eyes* (United States, Canada, Australia, New Zealand and the United Kingdom) in the EU. But France maintains close relations, which have been tightening steadily since 2009, with Washington and London in the nuclear, naval and air domains. The operational capacities of Paris, especially for first entry and in-depth strikes, are directly correlated to those of London and especially of Washington. In other words, while France criticizes, politically, the digital domination imposed by Washington on the Europeans, it benefits in part,

105. Interview, December 2017.
106. A. Pannier, "La France et ses alliés les plus proches : évolutions, opportunités et défis d'un engagement multiple" *[France and Its Closest Allies: Changes, Opportunities and Challenges of a Multiple Engagement]*, *Les Champs de Mars*, No. 30, 2018, pp. 9-17.
107. SGDSN, *Revue stratégique de cyberdéfense [Strategic Review of Cyber Defense]*, *op. cit.*, p.39.
108. *Ibid*., p. 40.
109. Ministry of Armies, *Revue stratégique de défense et de sécurité nationale [Strategic Review of Defense and National Security]*, October 2017, pp. 61-62.

operationally, in maintaining its military and security tool level in relation to its European partners, especially Germany. Conversely, although the necessity to strengthen ties with Berlin and encourage European strategic autonomy appears to be a political priority since the arrival at the Elysée of Emmanuel Macron, it is faced with both operational obstacles and a level of strategic ambition shared between Paris and Berlin.

Interviews conducted in Paris reflect this tension between privileged ties with London and privileged links with Berlin with regard to security data. They show, on the one hand, the extent to which the fight against terrorism is based on this data and, on the other hand, that it is at the heart of security policy. One official recommends that his authorities conclude a bilateral agreement with the United States as soon as possible, comparable to what they have with the United Kingdom in the name of "efficiency" since it would be too long to wait for an agreement in this particularly sensitive domain between the EU and the United States".[110] Another official justifies this approach as follows: "The subject today is terrorism; it is not the European project". And adds: "What more can be hoped for from an EU-28 agreement than a bilateral agreement in this domain, especially since the United States does not need an agreement since we are the ones who have problems with terrorism?" In his eyes, the control of security data reveals a cleavage between the European countries "with intelligence services that work" and the others.[111] For this cybersecurity specialist, it is the investments made to the benefit of its information services, beginning in 2007, that have allowed France to gain credibility with London and Washington and establish cooperation in certain fields.[112]

In the domain of data, the relationship with the United States remains decisive for all Europeans. For a country like France, the challenge is to reconcile a political criticism on the nature of this relationship and operational cooperation. The real convergences with Germany come up against Berlin's level of operational ambition. Inevitably, this focus on the United States is likely to continue to polarize the debate at a time when another leading tech power – China – is increasingly ambitious, as its strategy for *Big Data* or *Fintechs* shows, which aims to strengthen its state power.[113] On the external front, the BRI (*Belt & Road Initiative*) ultimately aims to reach the European market using rail and port infrastructure, but also digital.[114] This component is often overlooked even as major Chinese

110. Interview, November 2017.
111. Interview, December 2017.
112. Interview, January 2018.
113. J. Zeng, "China's Date with Big Data: Will it Strengthen or Threaten Authoritarian Rule?", *International Affairs*, No. 6, 2016, pp. 1443-1462.
114. M. Foucher, "L'Euro-Asie selon Pékin" *[Euro-Asia According to Beijing]*, *Politique étrangère*, Vol. 82, No. 1, 2017, pp. 106 and 109.

platforms are investing more and more in data centers across the EU. As one player in this sector observes, "the Europeans are caught in the noose".[115] That is why the EU's response, focused on the United States for obvious reasons, should also incorporate China's strategy: the geopolitics of data is not only transatlantic but increasingly Eurasian.

115. Interview, November 2017.

Conclusion

Highly complex and in movement, the geopolitics of data has, in the space of just a few years, taken rank on the international policy agenda. Control of data involves many players with very different contours and motivations: an issue of security and sovereignty for governments, it is a democratic issue for the people (personal data) and a fundamental challenge of creation of value for businesses. The recent *Cambridge Analytica* affair was precisely at the crossroads of these various issues, reminding us on the one hand of the response capabilities of states in the digital sphere, and on the other hand that the privacy of millions of individuals means little to the business strategies of the largest online platforms.

The mapping sketched out in this study, is informative in several respects. First, it reveals national data strategies taking different forms and partially nuancing the consensus arising from globalization. The United States has made data control the primary focus of both economic redevelopment structured around their tech giants and their national security strategy. These two elements combine in a long tradition of an open-door policy aimed at opening markets and maintaining American preeminence.[116]

China is in a state of uninhibited national power, through a long-term technological catch-up and a desire to break the Western digital and technological monopoly. In this context, data must make it possible to affirm the Chinese vision of cyberspace as well as to serve the "geopolitical instrument" of the "Silk Roads" project. Europe suffers from a double pincher effect: American hegemony and the Chinese assertion weaken the continent, which is struggling to position itself as a leading industrial power, therefore adopting an essentially defensive posture.

In 2018, the focus of data geopolitics must be shifted from the single transatlantic axis – it also concerns Asia. For Europe, the consequences of moving the center of gravity of the digital economy towards China – in a context of strong transatlantic tensions – are potentially significant.

Secondly, the definition of data, in particular "sensitive data", varies from one player to another.

116. D. McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet*, Basingstoke: Palgrave McMillan, 2015.

In terms of personal data, it is close to impossible to delimit a group of data universally recognized as "sensitive".[117] On the one hand, the respective traditions of individual states can lead to different classifications.[118] On the other hand, several approaches can be taken to isolate this type of data:

- an approach in terms of risk, adopted by the recent Chinese cybersecurity law;
- a contextual approach, adopted by American tradition, the same data being able to lose or acquire a sensitive character;
- a restrictive approach, adopted by European legislation, expressing in detail the different types of sensitive data.

In the absence of a common international approach to sensitive personal data, there is a risk of significant friction between the legal systems of the major digital players, particularly in the context of the various trade agreements currently being negotiated. The ability of a player to promote its own sensitive data protection standards will therefore depend on the weight of its economy, the dynamism of its digital ecosystem and a coherent political strategy. The European Union has so far preferred a legal and commercial approach to the issue by adoption of the GDPR, decisions on adequacy by the European Commission and inclusion of European standards in free trade agreements, with some success.[119] Nonetheless, faced with the competing regimes outlined in this study, it will not be able to do without a political ambition and a clean industrial strategy, at the risk of having its *soft power* crumble for lack of foundations.

Finally, the category of security data appears to acquire a specific rationale that is partly beyond that of personal data. Storage and circulation of it responds to more traditional mechanisms for protection of State secrets, alliance systems and strategic rivalry. For France, caught between the temptation of the P3 (United States, United Kingdom, France) in the field of intelligence and the need for Franco-German cooperation, the challenge is to go beyond the hiatus between political criticism coupled with a strong operational cooperation on the one hand, and a rhetoric of cooperation lacking a robust operational foundation on the other. A strengthened political, doctrinal and industrial collaboration in E3 format

117. Work by the OECD carried out in the 1980s already took note of this limit: "In fact, it is probably not possible to define a set of data that is universally considered sensitive." Annex to the Council Recommendation of September 23, 1980: Guidelines on the protection of privacy and transborder flows of personal data, Explanatory Memorandum, para. 19 a., OECD, 1980.
118. The Indian legislator raises the question of inserting caste membership into this category.
119. M. Scott et L. Cerulus, "Europe's New Data Protection Rules Export Data Privacy Standards Worldwide", *Politico*, February 6, 2018.

(France, United Kingdom, Germany) would perhaps be the appropriate combination to loosen what we called the "European noose": solving the political dilemma of the relationship with the United States while responding to China's emerging strategy. It is by finally considering the problem of data from the geopolitical and geoeconomic angles, and not merely legal and ethical, that Europeans will be able to actively contribute to the establishment of a real digital multipolarity that conforms with their interests and is compatible with their values.

ifri
institut français
des relations
internationales