EUROPEAN TECHNOLOGICAL SOVEREIGNTY

JANUARY 2022

RENAISSANCE numerique

TABLE OF CONTENTS

KEY TAKEAWAYS

THE QUESTION RAISED IS THAT OF THE EUROPEAN UNION'S STRATEGIC DEPENDENCE WHEN IT COMES TO DIGITAL TECHNOLOGY

- With the economy's and society's digital transformation, the quest for digital sovereignty goes beyond the mere scope of cyberspace. Digital transformation calls into question the autonomy of states' means of production and action, and their ability to ensure that their strategic interests are protected.
- In addition to the tensions inherent in the construction of the European Union, European sovereignty is faced with several sources of digital-induced threats: pressure from foreign states, infrastructural power of digital "super-platforms".
- The Covid-19 crisis called into focus the need not to depend on an extra-European "technology tap" for strategic technologies, i.e. not to run the risk of being cut off overnight from access to technologies that are essential for the European economy and society.

THE CONCEPT OF "SOVEREIGNTY" MUST BE CONSIDERED IN ITS ORIGINAL DEFINITION IN ORDER TO ESTABLISH A CLEAR OBJECTIVE FOR THE EUROPEAN UNION

- Sovereignty is a term historically linked to the state and its power to act in a given territory: the "power to be able".
- Strategic autonomy is both a means and a dividend of sovereignty.
- Digital sovereignty does not undermine classical sovereignty in its very physical conception of a state's territory: the territorial approach to digital sovereignty is particularly present in certain powers' strategies, whether they are authoritarian countries dealing with issues of territorial sovereignty in their more global geopolitical strategy (e.g. China and Russia) or states expressing their power through an extraterritorial presence (e.g. the American CLOUD Act).

DIGITAL TECHNOLOGY IS A NEW STRATEGIC DIMENSION

- Digital technology must be seen as a new strategic dimension, opened up by technological developments and through which the expressions of state sovereignty are conveyed and materialised. It thus complements land, sea, air, and space.
- However, digital technology is not a strategic dimension like any other, because it cuts across all the other dimensions. Its mastery allows states to confirm their sovereignty in the other strategic dimensions.

RENAISSANCE NUMÉRIQUE SUGGESTS DISCUSSING "TECHNOLOGICAL SOVEREIGNTY"

- Without technological expertise, there is no strategic autonomy in the digital field. Mastering the strategic digital technology aspect is not only a matter of digital technology, but also encompasses a number of other technologies, such as semiconductors.
- Certain technological layers of digital technology are prerequisites for guaranteeing sovereignty, and for each of them there is a critical threshold below which technological sovereignty is not ensured.
- Ranging from the raw materials needed to manufacture electronic chips, to the exploitation of digital services' usage data, these layers include a diversity of material strata and digital services.
- The policy aimed at guaranteeing technological sovereignty is a capacity building policy within a field of interdependencies, including the deliberate refusal or reduction of certain interdependencies in the name of a sovereignty objective. It is therefore about the European Union asserting its sovereignty without shutting itself off.
- In order to build industrial policies that promote its technological sovereignty, the European Union faces three possible scenarios: competition, coopetition, or cooperation.

FOR INVESTMENT CAPACITY REASONS, TECHNOLOGICAL SOVEREIGNTY CAN ONLY BE ACHIEVED AT EU LEVEL

- Historically, the technological sovereignty objective called for massive investments to master entire technological chains (cf. weapons, nuclear, space).
- The European Union must be considered here as a leverage of power for the Member States.
- Therefore, in terms of technological sovereignty policy, the principle of subsidiarity enshrined in European Union law should prevail.

THE EU NEEDS TO THINK ABOUT THE "PUBLIC/PRIVATE" RELATIONSHIP IN A STRATEGIC MANNER

- The ability of a local or regional authority to export its technologies is a means of ensuring not only its technological sovereignty, but also a leverage of power *vis-à-vis* its international counterparts.
- The European Union, like most of its Member States, has not yet succeeded in freeing itself from an administrative and legal conception of the role of public power, combining rigid theorising of what the "state" should or not do, and a tendency to mistrust private stakeholders.
- This relative distrust of economic power still hinders the advent of a partnership method of European power, which should necessarily combine public and private interests and stakeholders.
- The EU must now – like the rest of the world – develop its economic, legal, and administrative expertise in a strategic dimension, and integrate the independence of its sectoral and transversal regulators with the affirmation of its strategic objectives.

INTRODUCTION

IN SEARCH OF A SHARED DEFINITION

A CONCEPT THAT IS INCREASINGLY PRESENT IN EUROPEAN POLITICS

The concept of “digital sovereignty”, once used by a handful of stakeholders, has now entered the rhetoric at the highest level of European politics. Recent statements by the European Commission and Council testify to this growing willingness to make it tangible. In her State of the Union address in September 2020, European Commission President Ursula von der Leyen positioned digital sovereignty as a challenge for the European Union (EU)[1]. The ‘Digital Compass for 2030’, presented by the European Commission in March 2021, contributes to this objective[2]. The conclusions of the European Council of 1 and 2 October 2020 are also part of this process[3].

The acknowledgement of this challenge by the Member States and the European institutions has been a slow process. Two events in particular have contributed to this heightened awareness: the Edward Snowden revelations and the recent health crisis. In 2013, whistle-blower Edward Snowden revealed the extent of the surveillance of foreign states and institutions by US intelligence agencies, including the European Council. In terms of the methods used (spying on computer equipment, submarine cables, etc.), this affair highlighted the dominant position of the United States in the technological infrastructure sector[4], in particular operating systems and mass services platforms. It revealed that the US has the capacity to collect sensitive data in many states.

The other significant event was the Covid-19 crisis, that started in 2020. This crisis highlighted the strong dependence of Member States on other states for essential products, particularly in the health sector. This strategic dependence

[1] European Commission, “State of the Union Address by President von der Leyen at the European Parliament Plenary”, 16 September 2020: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

The Commission President reiterated this in her State of the Union address in September 2021, referring to the issue of “*European technological sovereignty*” mentioning that we should put “*all of our focus on it*”. European Commission, “2021 State of the Union Address by President von der Leyen”, 15 September 2021: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, “2030 Digital Compass: the European way for the Digital Decade”, 9 March 2021: https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF

[3] In these conclusions, the Member States refer to the objective of “*ensuring our technological sovereignty*”, or the importance for the European Union to “*be digitally sovereign*”. European Council, “European Council Conclusions, 1-2 October 2020”: https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/

[4] For more information, see the related article on Wikipedia: https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

was also an eye-opener for other industries. During the crisis, digital technology provided some resilience to the economy and society. Digital services and tools were put to the test. Those that proved their reliability in the face of such a surge significantly strengthened their grip. The crisis revealed how essential they were and how dependent Europeans were on them. It highlighted the need not to depend on a non-European "technology tap" for critical technologies, i.e. not to risk being cut off overnight from access to technologies that are essential for the European economy and society. It is interesting to note, in this respect, that China prefers the term "self-sufficiency" to "autonomy", reflecting its desire to no longer be tied to foreign products and services.

> *With the Covid crisis, the notion of scarcity emerged in political debates, and this is where the need for sovereignty, in terms of access to products and technologies, has become stronger in collective perceptions. [...] The risk of a significant shortage of digital goods has become palpable, and with it the risk of affecting the overall stability of the economy and society, as digital technology affects everything.*
>
> Thibaut Kleiner,
> Director, Policy Strategy and Outreach, DG CNECT, European Commission[5]

[5] Interview carried out in January 2021 as part of the Renaissance Numérique working group on European digital sovereignty.

> *For us, in the German government, this has always been a discussion about capacities to follow through with our own policy, abilities to act. We have seen, in the last couple of years, that the availability, the integrity and the deployment of a certain number of key technologies are gradually defining the capacity of States to act.*
>
> Nico Geide,
> Policy Planner for Digital Issues, German Federal Foreign Office[6]

Thus, digital transformation is reshuffling the cards of sovereignty. It calls into question the autonomy of the European Union's means of production and action, and its capacity to ensure that its strategic interests are upheld in the event of geopolitical tensions. In so doing, it leads European states to review the very concept of allies[7].

A DISCURSIVE TOOL THAT IS SUFFERING FROM A LACK OF DEFINITION

The concept of "digital sovereignty" is nevertheless struggling to emerge from its discursive dimension. Increasingly present in the public debate, it remains vague and encompasses a plurality of perceptions specific to the stakeholders who decide to use it. Originally a legal concept, it is now becoming a practical

[6] Interview carried out in March 2021 as part of the Renaissance Numérique working group on European digital sovereignty.

[7] This observation was made by researchers Alix Desforges and Didier Danet (quote translated from French): "*faced with unabated cyber espionage, including among allies, and the manipulation of personal data and information on major platforms, European states have realised that they cannot rely on foreign technologies and digital services*". Danet, D., Desforges, A., « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », Hérodote, 2020/2-3 (N° 177-178), p. 179-195. DOI: 10.3917/her.177.0179. URL: https://www.cairn.info/revue-herodote-2020-2-page-179.htm

political one, which is sufficiently broad for each stakeholder to interpret it in the way they wish to. While the geopolitical context highlights the need to address this issue, rigorous work must be undertaken in order to establish a definition. This is what Renaissance Numérique is trying to do in this note. The think tank's working group dedicated to "European digital sovereignty" has compiled an initial state of the art of academic and institutional publications on the concept of "digital sovereignty". It shows that very few authors actually undertake rigorous preliminary work with regards to defining terms, and instead focus on avenues of action before setting objectives. The different visions developed by the various stakeholders are not aligned in their scope, implications, or even in relation to the terms. This concept also sometimes competes with others, such as "strategic autonomy", despite their overlap.[8] A survey published in March 2021 by the Jean Jaurès and Friedrich Ebert Foundations illustrates the vagueness that exists around the concepts of "sovereignty" and "European sovereignty", and the great disparity of perceptions between Member States.[9]

"DIGITAL" AND "EUROPEAN": TERMS THAT POSE A DOUBLE CHALLENGE REGARDING DEFINITION

If current discussions are struggling to give a clear meaning to the concept of "sovereignty", which is nevertheless the subject of a well-established legal definition[10], the task is made even more difficult when it comes to defining the concept of "European digital sovereignty". The two terms associated with the word "sovereignty" are themselves subject to definitional issues. With regard to the use of the term "digital", it is worth considering what is meant and thus what it refers to: cyberspace or the different technological layers of digital technology? Moreover, when associated with sovereignty, the term can have two meanings. Does it refer to sovereignty within digital technology or to the impact of digital technology on sovereignty? With regard to the concept of "European sovereignty", it is part of a tension inherent in the construction of Europe, in other words, whether it is possible to consider it knowing that sovereignty is a concept directly linked to the state.

DIGITAL SOVEREIGNTY AND DIGITAL POLICY: FREQUENTLY CONFUSED TOPICS

Since the concept of digital sovereignty remains unclear, it has not been a real topic in digital public policy. More often than not, stakeholders start by designing digital policy before defining the objective of digital sovereignty. The broad scope of the French parliamentary mission's report *« Bâtir et promouvoir une souveraineté numérique nationale et européenne »*[11] ("Building and promoting national and European digital sovereignty") is an illustration of this.

Digital sovereignty and digital policy are not the same thing. Digital public policy can help build or strengthen digital sovereignty. Digital sovereignty, on the other hand, gives states the freedom to define their digital policy.

That is why it is important to distinguish between policies that ensure digital sovereignty and protectionist digital policies. Policies that guarantee digital sovereignty are policies of capacity building in a field of interdependencies, including the deliberate refusal or reduction of certain interdependencies in the name of a sovereignty objective. It is therefore a question of the European Union asserting its sovereignty without shutting itself off. In this respect, the European Commission recently used the idea of "*open strategic autonomy*"[12]. Behind these challenges lies the question of the acceptable level of dependence for Europe: below what threshold of digital dependence does the EU lose control of its sovereignty?

[8] On this subject, see section "The relevance of using the term "sovereignty" of this note, pp. 15-16.

[9] It was carried out by Ipsos among 8,000 European citizens in eight countries (France, Germany, Italy, Spain, Poland, Latvia, Romania, Sweden). « De la souveraineté européenne », Fondation Jean Jaurès and Fondation Friedrich Ebert, 1 March 2021: https://www.jean-jaures.org/publication/de-la-souverainete-europeenne/

[10] Refer to the first part of this note on this point.

[11] French National Assembly, « N° 4299 tome 1 - Rapport d'information de M. Philippe Latombe fait au nom de la mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » », 29 June 2021: https://www.assemblee-nationale.fr/dyn/15/rapports/souvnum/l15b4299-t1_rapport-information

[12] European Commission, "2021 Strategic Foresight Report. The EU's capacity and freedom to act", 8 September 2021: https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2021-strategic-foresight-report_en

PART 1
A NEW STRATEGIC DIMENSION

THE RELEVANCE OF USING THE TERM “SOVEREIGNTY”

In this definition exercise, Renaissance Numérique advocates for the use of the term “sovereignty” in its strictest sense. Far from the negative connotation that is frequently attached to it in France, associating it with nationalism or protectionism, the think tank encourages the consideration of this term according to its original meaning in order to establish a clear objective for the European Union.

Sovereignty is a term historically linked to the state and its power to act on a given territory: the “power to be able”[13]. In international law, it is defined as the ability of a state to assert its own existence and will within and outside its territory. Externally, the state of sovereignty is then based on a principle of mutual recognition.[14]

Debates often confuse “sovereignty” and “strategic autonomy”, with their respective torchbearers. While the concepts of sovereignty and strategic autonomy are closely intertwined, they are not at the same level. Strategic autonomy is both a means and a dividend of sovereignty. Unlike independence, it allows us to consider the state of globalisation and the constraints inherent in the interdependence of production chains. The idea of strategic autonomy is directly imported from the defense sector, particularly from France: *“Strategic autonomy is seen as the means for a state to exercise its sovereignty [RS2017; LBDSN 2008, 2013]. It aims to have an “autonomous capacity for assessment, decision, and action” ”.*[15] [16] For a state to be sovereign, this capacity must be irreducible,

[13] *“Originating in political philosophy, where it is restricted to the idea of national sovereignty, sovereignty can be defined as the capacity of an entity to set itself its own rules or, more trivially, as ‘the power to be able’”*. Ganascia, J.-G., Germain, E., Kirchner, C. (2018), “Sovereignty in the Digital Age. Keeping control over our choices and values”, CERNA: https://www.allistene.fr/files/2018/10/55710_Sovereignty_CERNA_2018.pdf

[14] According to Pierre Avril and Jean Gicquel sovereignty *“means, negatively, the absence of any external dependence and of any internal impediment. Positively, [it] designates the supreme nature of state power, and this power itself, i.e. the effective powers included in the power of the state. Sovereignty thus entails both independence in the international order (state sovereignty), exclusive power without limits other than those which the rule of law assigns to itself, in the internal order (sovereignty within the state), and the content of this power ”* (quote translated from French). Avril, P., Gicquel, J., *Lexique de droit constitutionnel*, Paris, PUF, 2003.

[15] Quote translated from French. Danet, D., Desforges, A., *op. cit*

[16] This approach is in line with other definitions of strategic autonomy. Paul Timmers proposes the following definition: *“Strategic autonomy is the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one’s longer-term future in the economy, society and their institutions”*. Timmers, P., “Cybersecurity is forcing a rethink of strategic autonomy”, OXPOL, 14 September 2018: https://blog.politics.ox.ac.uk/cybersecurity-is-forcing-a-rethink-of-strategic-autonomy/#cybersecurity%20%20#strategic_autonomy%20#sovereignty

hence the need to think clearly about digital sovereignty now that digital technology has become a *sine qua non* condition of the "power to be able" and is almost exclusively privatised.[17]

> *Many see the issue of sovereignty as a question of hegemony. But we see it as a question of strategic autonomy.*
>
> Henri Verdier,
> French Ambassador for Digital Affairs[18]

SOVEREIGNTY WITHIN DIGITAL TECHNOLOGY OR THE IMPACT OF DIGITAL TECHNOLOGY ON SOVEREIGNTY?

The concept of "digital sovereignty" could have two meanings, and address both a sovereignty issue within cyberspace and the impact of digital technology on sovereignty.[19] However, if we apply the strict definition of sovereignty linked to the state and its "power to be able" over what it considers to be its territory, then the second interpretation proves relevant and is used here.

[17] As an extension to the digital field, Resa Mohabbat Kar and Basanta E. P. Thapa define strategic autonomy as: *"the ability of the state to implement its own political, social and economic priorities, without being restricted to an undesired extent by external dependencies"*. Mohabbat Kar, R., Thapa B. E. P., "Digitale Souveränität als Strategische Autonomie", Kompetenzzentrum Öffentliche IT, September 2020: https://www.oeffentliche-it.de/publikationen. Quoted in Christakis, T., "European Digital Sovereignty": Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy", 18 December 2020: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098

[18] Interview carried out in January 2021 as part of the Renaissance Numérique working group on European digital sovereignty.

[19] On this subject, refer to Pierre-Yves Quiviger, « Une approche philosophique du concept émergent de souveraineté numérique », *Nouveaux Cahiers du Conseil Constitutionnel* n° 57 (Dossier: Droit constitutionnel à l'épreuve du numérique), October 2017: https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/une-approche-philosophique-du-concept-emergent-de-souverainete-numerique

The author mentions, in particular: *"The main difficulty with the concept of digital sovereignty lies in the ambivalence of a formulation to which the French language allows two meanings to be attributed: sovereignty over digital technology, digital technology then being what sovereignty relates to, or the field in which sovereignty may encounter a limit or have a tendency to manifest itself more resolutely (or not) [. ...] another meaning of the expression "digital sovereignty", namely, in a minimalist sense, the digital expressions of sovereignty (the difference is small but not negligible compared to the first sovereignty, which concerns digital matters)"*. Quote translated from French.

With the economy's and society's digital transformation, the quest for digital sovereignty goes beyond the sole perimeter of cyberspace.

Given its cross-functional nature, digital transformation affects the exercise of sovereignty in multiple dimensions: economy, food[20], health, culture, education, defence, security[21], etc. It influences the very nature of political regimes[22]. It is eroding sovereignty in the most traditional sense of the term: can the European Union still make – i.e. adopt and enforce – the rules it wants?

Beyond the tensions inherent in the construction of the European Union[23], European sovereignty is exposed to several sources of digital threats. The EU is up against foreign states that are capable of carrying out cyberattacks or cyberespionage against its institutions or Member States, or of using the "technology tap" as a way to exert pressure. Digital "super-platforms"[24] are encroaching on the states' powers. Although their power is not absolute, these companies combine components inherent to sovereignty. Researcher Henri Isaac refers to their "infrastructural power"[25]. They define the boundaries of spaces that play a part in the democratic and state arenas and impose their own standards and vocabulary. They promote their own language through their services. They are able to reach out to populations more extensively than governments themselves and thus influence the political field in the direction of their economic and societal models. They are developing massive data collection and analysis capabilities for their own purposes, which may be unparalleled by individual states. They therefore pose a challenge to the power of states, as these capabilities are not easy to build. The strengthening of the

[20] The collection of agricultural data, for example, has become a sovereignty matter. See Bounaud, P., Pouyat, M., « Données agricoles en Europe : défendre notre valeur commune », Renaissance Numérique, tribune, 21 May 2019 : https://www.renaissancenumerique.org/publications/donnees-agricoles-en-europe-defendre-notre-valeur-commune

[21] In this respect, Alix Desforges and Didier Danet point out that: *"the digital revolution has effectively changed the way this sovereignty is exercised because it allows cross-border operations and also because it offers remote means of action to spy on and sabotage networks by concealing one's identity and hiding behind multiple jurisdictions"* (quote translated from French). Danet, D., Desforges, A., *op. cit.*

[22] To stretch the point, liberal regimes have to protect themselves against the interference of information bubbles, while authoritarian regimes have to protect themselves against the free flow of information.

[23] See section "Is European Technological Sovereignty Possible?" in this note, pp. 28-35.

[24] This term is defined by the researcher Henri Isaac and refers in particular to the following stakeholders: Google, Facebook, ByteDance, Tencent, Microsoft et Alibaba. H. Isaac, (2021), « L'irrésistible montée en puissance des super-plateformes numériques », Questions Internationales, n°109, September.

[25] On this subject, Henri Isaac proposes an analysis of the power of digital "super-platforms" based on Michael Mann's distinction between states' "despotic power" and "infrastructural power".

Chinese state’s control over its digital giants illustrates this tension between states and these major tech players[26]. These different sources of threat can also overlap. In the field of intelligence, for example, public intelligence and private intelligence are mechanically intertwined. Moreover, these companies are non-European and sometimes have allegiances to their home country and are subject to extraterritorial legislation.

Although digital sovereignty is not limited to cyberspace, it doesn’t override traditional sovereignty in its very physical definition of a state’s territory[27]. The territorial approach to digital sovereignty is particularly present in the strategies of certain powers, whether they are authoritarian countries faced with questions of territorial sovereignty in their more global geopolitical strategy (e.g. China and Russia) or states expressing their power through an extraterritorial presence. In this respect, the American CLOUD Act is an extraterritorial projection of sovereignty which consists in presuming that, when services have been exported by technological or economic stakeholders considered to be attached to a sovereign state of origin, access by this state extends to all the data processed by these stakeholders wherever they may be in the world and, therefore, that the territorial application of the law has no other boundary than the capital-based link, even indirectly[28], to allow their recovery by the authorities of this state.

DIGITAL TECHNOLOGY AS A STRATEGIC DIMENSION

Digital technology must therefore be seen as a new strategic dimension, opened up by technological developments. The European Union’s strategy must be examined to see whether and how it intends to acquire the necessary digital resources and levers for action to guarantee its sovereignty. Digital technology is a fifth strategic dimension, in addition to land, sea, air, and space, through which the expressions of state sovereignty are conveyed and materialised. It is therefore important to identify the specific features of this new dimension.

The emergence of air and space domains in states’ strategies (thanks to technological advances that have made them areas of power) constitutes a relevant example for understanding the issues linking sovereignty to digital technology. Airspace and outer space call territory representations into question. In addition to other already mastered strategic dimensions (sea, land), they have a specific function. In both air and outer space, the theoretician Hervé Coutau-Bégarie emphasises a double central phenomenon that redefines the balance of power between stakeholders in the strategic arena: *“the dilation of space and the shrinking of time”*. Airspace has enabled the *“unification of strategic spaces”*, creating new intermediation mechanisms with a reduction in the time needed to connect stakeholders in the strategic arena. With space, this double phenomenon is materialised, for example, through the transformation brought about by satellites. It is thanks to these new technologies, according to the author, that Earth has become a *“truly unified theatre, which a centralised command can control in real time and continuously”* for the first time. According to Hervé Coutau-Bégarie, space intervenes in *“all components of strategy”*, but also in a different way. Indeed, the *“predominance of passive systems over active (or aggressive) systems”* in relation to other strategic dimensions is space’s main characteristic: *“Whereas the functions of land, sea, or air systems are primarily combat-oriented, space systems are oriented towards the See-Listen-Communicate triptych, i.e. towards observation and communication functions in support of other environments”*[29]. States have thus long ruled out the deployment of weapons in space, and use this dimension mainly for surveillance devices. In this respect, space still plays a stabilising role in the international order. The digital strategic dimension is also different from space, in that digital tools are subject to and are involved in many attacks. In this respect, it cannot be considered an active element supporting the stability of international order. It is a dimension worked from within by a principle of confrontation.

[26] «De Jack Ma à TikTok, pourquoi Pékin reprend le contrôle des géants de la tech chinoise», Bogdan Bodnar, *Business Insider France*, 26 May 2021 : https://www.businessinsider.fr/de-jack-ma-a-tiktok-pourquoi-pekin-reprend-le-controle-des-geants-de-la-tech-chinoise-187637

[27] French MP Philippe Latombe and the members of his parliamentary mission expressed it well in their report (quote translated from French): *“digital technology does not fundamentally call into question the sovereignty of states, it simply reshuffles the cards of power relations between them at the international level and constitutes a powerful lever of influence in the short and medium term”*. French National Assembly, *op. cit.*

[28] Companies subject to the CLOUD Act are those owned directly or indirectly by an American stakeholder.

[29] Coutau-Bégarie, H. (2011), *Traité de stratégie*, Economica, 7th edition.

Digital technology, a new power factor, is not a strategic dimension like any other. It is difficult to compare it with the previous strategic dimensions, as this would partly imply that digital technology is seen as a separate domain, whereas it cuts across all the others. Mastery of this dimension makes it possible to consolidate one's sovereignty in the other strategic dimensions. It also influences the existing relationships between the different strategic dimensions. This is made possible by the development of new forms of intermediation. Grégoire Germain and Paul Massart illustrate this specific role through the example of digital infrastructures which *"are developing on land (servers), at sea (submarine cables), in the air, and in exo-atmospheric space for certain space segments, notably in terms of military combat systems"*.[30] Moreover, digital technology is a strategic dimension characterised by its ability to expand, unlike other dimensions.

[30] Germain, G., Massart, P., « Souveraineté numérique », Études, 2017/10 (Octobre), p. 45-58. DOI : 10.3917/etu.4242.0045. URL : https://www.cairn.info/revue-etudes-2017-10-page-45.htm

PART 2
FROM DIGITAL SOVEREIGNTY TO TECHNOLOGICAL SOVEREIGNTY

MASTERY OF THE DIGITAL STRATEGIC DIMENSION IS BASED ON MASTERY OF DIGITAL TECHNOLOGY'S TECHNOLOGICAL LAYERS

Defining a clear objective for the European Union requires being precise regarding which terms are used. In order to invest in a new strategic dimension (in this case, digital technology), one must not be dependent on the external environment. However, mastery of the digital strategic dimension is not only a matter of digital technology, but also encompasses a number of technologies, such as semi-conductors[31]. Without technological mastery, there is no strategic digital autonomy. This is why Renaissance Numérique suggests talking about "technological sovereignty" rather than "digital sovereignty".

> *Some of the technologies relevant here are not digital, like quantum computing for example. 'Digital' is not the concept we use. 'Technological sovereignty' is the term we use. 'Technological sovereignty' is the ability to develop, to deploy, to apply, to source and guarantee the integrity of a number of key technologies that have become instruments of power in this time of geopolitical competition that we live in. The most relevant ones might be AI, cloud computing, semi-conductors and the whole value chain that comes with them.*
>
> Nico Geide,
> Policy Planner for Digital Issues, German Federal Foreign Office[32]

[31] For more information, see the related page on Wikipedia: https://en.wikipedia.org/wiki/Semiconductor

[32] Interview carried out in March 2021 as part of the Renaissance Numérique working group on European digital sovereignty.

For the European Union, it is a matter of verifying the conditions for guaranteeing a state of sovereignty. Sovereignty is at stake in some of digital technology's technological layers, from the raw materials needed to manufacture chips, to the use of data in digital services. The majority of powerful stakeholders seek an integrated model, i.e. vertical control of these layers. The EU has strengths in some of the technology layers, but does not master all of them in a way that would make it independent. It cannot, by itself, possess all the elements that make up each layer, especially as digital technologies are often open-ended in nature. Nevertheless, there are ways in which it can achieve a greater degree of control over these different layers in the future, either by strengthening its production capacity or by other means.

DEEP TECH IS NOT THE ONLY LEVER FOR TECHNOLOGICAL SOVEREIGNTY

This process of identification is important and should make it possible to establish relevant strategies far from the incantations in favour of building European digital giants. This does not mean that this objective cannot be part of a strategy to guarantee European technological sovereignty. But to find out, it is worth defining what is necessary in order to guarantee strategic sufficiency in the event of a low or high intensity crisis. Certain technological layers are prerequisites for ensuring sovereignty, and for each of them there is a critical threshold below which technological sovereignty is not ensured. These layers don't necessarily correspond to deep tech, and include a variety of hardware layers and digital services[33]. The challenge is to identify these critical layers and thresholds of dependence, to know where the EU stands in these different areas, and to build industrial policies in order to achieve them.

The EU is therefore faced with three scenarios: competition, coopetition, or cooperation. The first scenario (competition) consists of creating European digital champions to compete with the major existing players or to build the major competitors of tomorrow. This scenario requires substantial public and private investment and organised ecosystems to encourage the emergence of these players. It is therefore often a medium to long-term scenario.

The second scenario (coopetition) consists of building industrial alliances between existing European private players. It is about identifying which players are getting close to the targeted critical thresholds and thinking about their alliance so that they can gain market shares. From this point of view, the European Union could also encourage investment policies to take over technological bricks that exist abroad, as non-European players have been able to do in Europe.

Finally, the third scenario (cooperation) consists of breaking out of the proprietary logic established until now by certain major tech players and forcing strong interoperability of strategic technologies by imposing shared standards. GAIA-X[34] fits straight into this scenario. This initiative is to be welcomed, in the sense that it shows that the need for a common approach at European level has been identified. However, it has vulnerabilities linked to a lack of maturity in its implementation, as illustrated by the membership conditions which are essentially based on a territoriality criterion and do not take into account the players' nationality. This path does not completely eliminate the problem of dependence, since it embodies the state of European supply in relation to its global competitors. This project, which was intended to be sovereign, demonstrates the current incompleteness of what Europe has to offer in this area – due to the lack of integration between infrastructures and services – since it only allows for the creation of an integrated chain of infrastructures and services by welcoming non-European players who will fill the gaps not satisfied by a fragmented European offering. This leads GAIA-X to miss its target – and the French National Agency for the Security of Information Systems (ANSSI) to consider tightening its certification criteria[35] – given that the non-European players who take part in it are subject to the extra-territoriality of the laws and

[33] Renaissance Numérique is currently conducting a review of the technological layers of digital technology that have sovereignty implications for the European Union. This work, which is ongoing, covers a variety of layers such as raw materials, microprocessors, large digital platforms, Internet protocols and quantum computing (this list is non-exhaustive).

[34] For more information, see the project website: https://www.gaia-x.eu

[35] See in this respect the revision of the "SecNumCloud" reference framework. French National Agency for Information Systems Security (ANSSI), « Prestataires de services d'informatique en nuage (SecNumCloud). Référentiel d'exigences », Part « 19.6 Immunité au droit extracommunautaire », Version 3.2.a of 21 September 2021: https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a_revision.pdf

are at odds with the Schrems II ruling of the Court of Justice of the European Union (CJEU)[36], which makes it impossible to achieve the initial objective of a European "safe" that's free of any extra-European influence.

The French approach implemented by ANSSI had until now been based on the possibility of building offerings that were free of any legal influence from outside the European Union, without prohibiting the possibility of calling upon non-European players. The agency must now adapt to the "Schrems II" decision, which requires Member States, administrations, and European companies to avoid the effects in Europe of non-European countries' laws.

When these extra-territorial laws are imposed by the nationality of the main shareholder of a European subsidiary providing IT services, it is not enough to set up subsidiaries in Europe, or to host data in European data centres, or even to conclude IT contracts governed exclusively by local European law, or even to promise the European authorities that the injunctions to submit to extra-territorial laws to which the nationality of the parent company subjects its European subsidiary will be violated on first request.

The capitalistic link to a non-European "parent" company – American, for example – is now presumed to be problematic by European law. Even if this problem, which has arisen as a result of a CJEU decision, doesn't have an instant practical solution, it inevitably implies that the chains of IT services should be conceived in terms of the nationality of the companies and their shareholders, and no longer only in terms of the territoriality of the IT service provided or the establishment of a subsidiary and its IT infrastructure.

[36] Renaissance Numérique (2021), « Arrêt Schrems II : Comment sortir de l'impasse ? » : https://www.renaissancenumerique.org/publications/arret-schrems-ii-comment-sortir-de-l-impasse

PART 3
IS EUROPEAN TECHNOLOGICAL SOVEREIGNTY POSSIBLE?

Based on the way in which sovereignty has been defined here, it is possible to question the relevance of aiming for European technological sovereignty. In its conventional definition, the concept of sovereignty is linked to a national scale. How then can we consider it at a supranational level, in this case European, in the face of other more unified entities, be they centralised (China) or federal (United States)? This question relates to a typical problem of technological sovereignty (cf. armaments, nuclear energy, space), namely that, historically, the objective of technological sovereignty called for massive investments to master entire technological chains. The semi-conductor market is significant in this respect. It is a major concentration industry with massive capital, requiring decades of investment to produce the latest generation products. In the coming months, for example, the US is expected to allocate $52 billion in funding to subsidise the construction of state-of-the-art factories in the US[37]. Similarly, the total amount spent on research and development for digital “super-platforms” (excluding ByteDance) is equivalent to just over seven times the European research budget for the year 2020 (97.4 billion dollars versus 11`billion euros)[38]. These amounts can only exist on a European scale.

A TERM NOT MENTIONED IN THE EUROPEAN UNION’S FOUNDING TREATIES

Questions about the European nature of technological sovereignty are linked to questions about European construction and integration.[39] The European Union is a political entity which bases its construction on a principle of delegation of sovereignty and not of sovereignty. The term sovereignty does not appear anywhere in the treaties establishing the European Union[40] [41] unlike

[37] Eurasia Group, “EU/Geo-technology: Semiconductor push will cost billions, take years, and still not deliver self-sufficiency”, 4 November 2021.

[38] H. Isaac, (2021), *op. cit.*

[39] Pierre Avril and Jean Gicquel recall that from a constitutional point of view, sovereignty is *“the prerogative of the state, as opposed to an international organisation (European Union) which can only benefit from transfers of competencies agreed by the Member States”* (quote translated from French). Avril, P., Gicquel, J. (2003), *op. cit.*

[40] Christakis, T., *op. cit.*

[41] The European Union’s founding treaties are listed on the European Union law website, EUR-Lex: https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-founding.html?locale=en

national constitutional texts such as the French Constitution, which refer to "national sovereignty"[42]. The current state of the debate on the legal structure of the European Union is not conducive to the legal establishment of European sovereignty. However, it is already a tangible geopolitical and democratic issue that reflects its member states' sovereignty challenges.

DIVERGENCES BETWEEN MEMBER STATES

But is it possible to achieve technological sovereignty at European level given these integration challenges and the prerequisite of a common political willingness among Member States to embark on this path? Currently, there is no shared vision on the use of the "European technological sovereignty" concept and what it encompasses.

Not all Member States have formally taken a position on the development of European technological sovereignty, and those that do agree on the need for it do not do so in the same terms and/or with the same level of ambition[43]. Depending on the maturity of their digital economy and their socio-cultural history, Member States do not have the same level of interest in this[44]. The link between the Eastern European states and the United States in order to defend themselves against Russia, for example, contributes to these countries distancing themselves from the concept of European autonomy. Similarly, the level of the French and German digital economies compared to smaller European states contributes to the focus given to this issue in these countries.

[42] French Constitutional Council, « Texte intégral de la Constitution du 4 octobre 1958 en vigueur », Full text in force as of the constitutional revision of 23 July 2008 : https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur

[43] Alix Desforges and Didier Danet cite a study by the European Council of Foreign Relations think tank in 2019 which *"shows that not all Member States support the development of a European strategic autonomy and that those that do not agree on what it entails, nor "on the geographical and functional level of ambition they should adopt" to implement it"*. Danet, D., Desforges, A., *op. cit.*

[44] French National Assembly, *op. cit.*

TECHNOLOGICAL SOVEREIGNTY QUESTIONS THE EUROPEAN UNION'S "POWER TO BE ABLE"

Raising the question of technological sovereignty leads to questions about the reality of the European Union's "power to be able". Can the EU be powerful without the traditional attributes of sovereignty? In some respects, the EU already possesses some elements of digital power, notably through the regulation of the digital economy. This regulatory power is expressed in the Union's ability to sanction the violation of its own rules by non-European players and also to locally sanction violations of its own rules by Member States. It is also expressed through the recognition of this power abroad. Professor Anu Bradford has theorised this recognition through the concept of the "Brussels effect"[45], which illustrates the EU's ability to inspire foreign regulations. One of the most frequently cited examples is the General Data Protection Regulation (GDPR). However, if the latter demonstrates the EU's capacity to build an extraterritorial projection of its law, this regulation was not conceived as an instrument of power, but rather as a tool to protect European citizens. The GDPR also illustrates that this type of "legal power" can be relatively limited when "code is law", as Lawrence Lessig[46] famously put it. The implementation of the regulation by Google – with the Privacy Sandbox[47] – and Apple – with the App Tracking Transparency[48] – is, in this respect, illustrative, as these players impose, through their infrastructure, their own standards on their ecosystem to comply with the European framework.

Moreover, the enforcement of this law remains defensive and only upholds itself *a posteriori*, in a marginal way. It depends on its judicialisation and a judge's independent interpretation. With the Schrems II judgment, for example, the Court of Justice of the European Union gave data protection a political direction that no Member State had given until now, by finding that an IT service provider was subject to extra-territorial laws that had an effect

[45] Christakis, T., *op. cit.*

[46] Lessig, L. (2000), "Code is law, On Liberty in Cyberspace", *Harvard magazine*: https://www.harvardmagazine.com/2000/01/code-is-law-html

[47] For more information, see their website: https://privacysandbox.com

[48] For more information, see their website: https://developer.apple.com/documentation/apptrackingtransparency

on its European subsidiaries and IT services. This decision now applies as a new rule, without any European legislator having made a firm political choice. At the same time, in October 2020, the same Court of Justice invalidated, in the "French Data Network and others"[49] ruling, the European texts – and, by extension, the national laws – that had been in force since 2002 in Europe (and 2001 in France) governing the retention and judicial and administrative requisitioning of "traffic data" generated by the use of the services of Internet access providers, telecom operators and hosting providers. Some people are pleased that the requirement for proportionality and transparency in security laws has finally prevailed over the "security/freedom" balance that has until now been reached by parliamentary majorities under the control of their constitutional courts. Some point to the paradox of not subjecting public security policies to European law, but deconstructing them *a posteriori* through the case law of the CJEU inspired by the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms.

This judicialisation does not build European power or growth. Moreover, the undeniable inspiration of European law is reinterpreted by foreign sovereignties erected to defeat European law. For example, China's new Personal Information Protection Law (PIPL), which came into force on 1 November 2021, establishes a powerful body of rules presented as encouraging individual citizen consent – inspired by the GDPR – and linked with prior administrative authorisation and the obligation to locate servers and data in China, showing that it is possible to be emulated by strategies that are opposed to our objectives or values. These initiatives raise questions for the European Union, whose power seems to be materialised only by the law resulting from the disputes referred to its supreme courts, according to circumstantial and category-based interests.

This power to regulate the digital economy is itself limited and is struggling to bring about technological sovereignty. The European Union is a political entity that was built around issues closely linked to the regulation of markets and competition law, and which is now faced with a partly privatised and oligopolistic Internet in terms of technological sovereignty. While this issue concerns any major power that must also reconsider its regulations, this challenge has taken on particular characteristics for the EU. Its legal architecture constrains its own regulatory power. In this respect, Professor Theodore Christakis reminds us of the barrier posed by the unanimity vote, which often makes it difficult to obtain an agreement between the Member States. This was the case for the debates on the taxation of digital services, taxation being a field where unanimity is required. The academic points out that this difficulty also arises on decisions based on majority voting, taking the example of the E-evidence Regulation.[50]

Beyond voting procedures, the EU's technological sovereignty is hampered by the fact that national security remains a prerogative of the Member States.[51] Moreover, not all Member States have the same conception of it. In digital matters, there are, for example, conceptual differences regarding the processing of data related to national security, particularly with regard to the control that must be exercised. On this point, Theodore Christakis considers that the series of judgments of the Court of Justice of the European Union of 6 October 2020 concerning government access to communications data has taken part in the erosion of the national security exemption.[52] However, while this case law has weakened national sovereignties by requiring Member States to comply with the criteria of European human rights law, it has not strengthened European sovereignty. Paradoxically, the interference of European law in national security strategies has the immediate effect of dissuading the desire for a European security model.

The current debates in the European Union show more generally that not all Member States have the same approach (and sometimes the same respect) for the rule of law. Security links between Member States and non-Member States are thus often bilateral and may differ between Member States. These divergences were recalled by researcher Marietje Schaake during the European

[49] Judgment of 6 October 2020, Joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others v Premier ministre and others.: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0511

[50] Christakis, T., *op. cit.*

[51] There is a legal limit to how far the EU can exercise its regulatory power over national security issues. According to Article 4(2) of the Treaty on European Union, *"The Union shall respect [the Member States'] essential State functions, including [...] safeguarding national security. In particular, national security remains the sole responsibility of each Member State".*

[52] T. Christakis, *op. cit.*

conference organised by Renaissance Numérique in May 2021 on European digital sovereignty: *"These two areas* (the European single market and national security) *are currently in conflict with each other: there is the promise of a digital single market in Europe, but there are twenty-seven different authorities to assess whether national security is at stake. This was highlighted when they had to consider whether Huawei and other network technologies were safe enough to be used in Europe."*[53]

This issue is intertwined with that of the common defence policy, which is struggling to be constructed for lack of a shared vision of the European Union's power. If the EU is not capable of having a common defence project, it will be difficult for it to have a sovereignty project – whether this defence and sovereignty are digital or not. The strong influence of the United States through the North Atlantic Treaty Organisation (NATO) in Europe plays a significant role in this constraint, at a time when the control of submarine cables in French territorial waters depends on discussions within NATO[54].

TECHNOLOGICAL SOVEREIGNTY THAT CAN ONLY BE ACHIEVED AT A EUROPEAN LEVEL?

It is now time to overcome these barriers, because technological sovereignty cannot exist for the Member States if it's not European. Due to investment capacity, technological sovereignty can only be achieved at Community level. In this context, the European Union must be seen as a lever of power for the Member States.[55]

The principle of subsidiarity enshrined in European Union law must therefore prevail. As the European Parliament points out, *"it* [the principle of subsidiarity] *only legitimises the Union's exercise of its powers where Member States are unable to achieve the objectives of a proposed action satisfactorily, and where action at Union level can provide added value"*[56].

The European Union has lived in denial about power issues for too long. Indeed, some Member States are opposed to a powerful Union. However, if Member States wish to guarantee their own technological sovereignty, they must accept the principle of subsidiarity in this area. Subsidiarity does not negate their national sovereignty. It is justified by their state of sovereignty and is reflected in a distribution of competencies.

In this respect, the European space history should inspire. Autonomous access to space has, from the outset, been seen as an element of sovereignty by important EU countries. Subsequently, the Galileo project was defined and implemented because the keys to signal degradation, synchronisation, dating, and GPS localisation were held by the US Pentagon. The recent history of space can also serve as an enlightening analysis. While new private players such as SpaceX, headed by Elon Musk, are gaining power, the opening-up of tenders by the US government, which therefore retains control, directly benefits them.

[53] Renaissance Numérique (2021), "Digital Sovereignty: Which Strategy for Europe?": https://www.renaissancenumerique.org/publications/digital-sovereignty-which-strategy-for-europe

[54] « L'OTAN veut protéger les câbles sous-marins des attaques russes », *Euractiv*, 23 october 2020 : https://www.euractiv.fr/section/politique/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

[55] French National Assembly *op. cit.*

[56] See the presentation on the European Parliament website: https://www.europarl.europa.eu/factsheets/en/sheet/7/the-principle-of-subsidiarity

CONCLUSION

THE EU NEEDS TO THINK ABOUT THE "PUBLIC/PRIVATE" RELATIONSHIP IN A STRATEGIC MANNER

If the Member States wish to guarantee their technological sovereignty, it can only be European. It is not a question of renouncing their national sovereignty, but on the contrary of strengthening it by giving themselves the collective means to do so. To achieve this, it is essential to overcome the confusion of terms, which does not allow for a clear and common vision of the objectives for the European Union.

Digital technology is a strategic dimension through which the territory of traditional sovereignty must be redefined. It is therefore necessary to establish the conditions of access to this dimension. Doing so requires analysing in-depth the various digital technological layers and determining the critical thresholds below which European technological sovereignty is not ensured.

The United States developed a strategic approach to the economy with the 'Information Superhighway', under Bill Clinton, and the adaptation of the 1974 Foreign Intelligence Surveillance Act (FISA) to digital technology, which includes in its definition of national sovereignty economic power and interests in the service of national power, particularly in international relations.

This economic conception of American "national security" is more than half a century old. It translates into convergences of valued public-private interests. Its application in support of economic and strategic interests considered to be "sovereign" is at the same time regulatory, judicial, diplomatic, and economic, and has never been confined to the supposedly regal domain of national defence and security, nor to the sole geographical territory of the United States. From the Small Business Act of 1953 – which embodies the economic affirmation of a national preference in emerging sectors – to the instrumentalisation of law and judges for the purposes of economic and strategic power, from the fight against corruption and money laundering, to the control of dollar transactions and foreign investments, via embargo policies, the American legal and judicial arsenal is resolutely an instrument for the extra-territorial projection of economic and political power, intended to defend and promote the interests of the United States internationally. This arsenal is made up of a chain of economic competencies that deeply influence the judicial, diplomatic, and regalian organisation of the federal state, well beyond the apparent economic regulators[57].

[57] See in this regard: Pierucci, F., Aron, M. (2019), *Le piège américain*, JC Lattès

With different political cultures and methods, China and Russia have also decided, over the last fifteen years, to instrumentalise the development framework of their economic and strategic hosts, using a very controlled approach to the strategic and sovereign interests – offensive and defensive – of technological power.

Thus, the ability of a local or regional power to export its technologies is a means of ensuring not only its technological sovereignty, but also a lever of power *vis-à-vis* its international counterparts.

While the objective of technological sovereignty requires massive and rapid investment, it is more than ever important for the EU to adopt a convergent approach that dictates political and economic agendas. However, until 2019, the interweaving of economic and technological issues was not thought through in terms of European sovereignty, including at Member State level.

One of the factors that may explain this lack of vision, and then of action, is not so much a question of competencies, as of method, which is itself the result of a political, judicial, and administrative culture. The understanding of the role of public action in these strategic issues has very often restricted the "state as protector" to the role of public fund provider or regulator of the excesses of economic power within the internal market. It was not until the first speeches by Thierry Breton, European Commissioner for the Internal Market, and the impetus of the 'Digital Compass for 2030'[58] programme, that a political vision of Europe's power deficit in the technology sectors was embodied in 2019. The global pandemic has given this impulse an ideological consolidation and broadening.

However, the European Union, like most of its Member States, has not yet succeeded in freeing itself from an administrative and legal conception of the role of public power, combining a rigid theorising of what the "state" should or not do, and a tendency to mistrust private stakeholders. This still dominant conception has deep roots in national and European cultures of power, which can be summarised as follows: if it is public, power should be independent of economic interests; if it is private, it should be curtailed in its excesses.

Basically, these two areas of expression of a relative mistrust of economic power are still holding back the advent of a partnership method of European power, which should necessarily combine public and private interests and stakeholders. To do this, the public authorities would have to admit that they should take greater advantage of the observation point of economic conflicts that the multiplication of their interactions with economic stakeholders would give them, beyond the punitive practice – judicial and administrative – of law. If this methodological opening were to be accepted, the relevance of public policies would be considerably strengthened.

It is also a question of European economic stakeholders having greater confidence in the diplomatic protection offered to them by European law outside the physical borders of the European Union. Such confidence cannot be imposed by decree. It is achieved through legislative, administrative, diplomatic, and judicial measures and not through speeches, however voluntaristic they may be.

The EU must now – like the rest of the world – develop its economic, judicial, and administrative competencies in a strategic dimension and combine the independence of its sectoral and transversal regulators with the affirmation of its strategic objectives.

Sovereignty is always imperfect[59], since its nature is to be contested according to permanent power relations. The same applies to technological sovereignty, which is constrained by the interdependencies inherent in the production of technologies. But sovereignty must be a permanent affirmation, because it cannot be shared.

[58] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *op. cit.*

[59] In the words of Stephen Krasner, quoted by: Pohle, J., Thiel, T. (2020), "Digital sovereignty", *Internet Policy Review*, 9(4). Accessible via https://doi.org/10.14763/2020.4.1532 and https://policyreview.info/concepts/digital-sovereignty

ACKNOWLEDGEMENTS

WE WOULD LIKE TO THANK THE VARIOUS STAKEHOLDERS WHO TOOK PART IN THE INTERVIEWS FOR THEIR CONTRIBUTION:

Daniela Battisti, Head of International Relations, Ministry of Technological Innovation and Digital Transformation, Italy

Godefroy Beauvallet, Head of the General Council Department, French General Economic Council (CGE)

Annie Blandin, Professor, "Network Systems, Cybersecurity and Digital Law" Department, ITM Atlantique

Christine Cabuzel-Duvallon, Deputy Head, "Internal Market, Industry, Research and Innovation, Digital Technology and Space" Sector, French General Secretariat for European Affairs (SGAE)

Joffrey Célestin-Urbain, Head of the Strategic Information and Economic Security Department, French Ministry of Economy, Finance, and Economic Recovery

Vice Admiral Arnaud Coustillière, Cyber and Digital Senior Advisor, Str@t-Algo

Raphaël de Cormis, "Digital Factory" Vice-President, Thales

Stéphane Dupuis, Deputy Secretary General for European Affairs, French General Secretariat for European Affairs (SGAE)

Laurent Ferrali, Director of Government and IGO Engagement, ICANN

Nico Geide, Policy planner for digital issues, German Federal Foreign Office

Thibaut Kleiner, Director, Policy Strategy and Outreach, DG CNECT, European Commission

Olaf Kolkman, Principal "Internet Technology, Policy, and Advocacy", Internet Society

Konstantinos Komaitis, Senior Director, "Strategy and Policy Development", Internet Society

Stefan Koreneef, Counsellor for Innovation, Science and Technology, Dutch Embassy in France

Tanguy Larher, "Internal Market, Industry, Research and Innovation, Digital Technology and Space" Sector Manager, French General Secretariat for European Affairs (SGAE)

Henri Verdier, French Ambassador for Digital Affairs

Suzanne Yountchi, Economic Officer for Trade, Digital Economy and Cybersecurity, US Embassy in France

AUTHORS

Jennyfer Chrétien, Executive Director, Renaissance Numérique

Etienne Drouard, Partner, Hogan Lovells (Paris) LLP

THE WORKING GROUP

Guillaume Buffet, President, U Change

Lucien Castex, Public Affairs and Partnership Development Representative, AFNIC

Arnaud Dechoux, European Public Affairs Manager, Kaspersky

Pierre-Frédéric Degon, Government Affairs Manager, Abbott France

Hector de Rivoire, Government Affairs Manager, Microsoft France

Etienne Drouard, Partner, Hogan Lovells (Paris) LLP

Anne Duboscq, Public Affairs Director, OVHcloud

Olivier Esper, Head of Institutional Relations, Google France

Valérie Fernandez, Professor and Chair for "Responsibility for Digital Identity", Telecom Paris

Henri Isaac, Associate Professor, PSL Université Paris-Dauphine

Julie Lavet, Government Affairs Manager, Apple France

Samuel Le Goff, Consultant, CommStrat

Emmanuel Lempert, Vice President, Government Affairs for France, MENA and French Speaking Africa, SAP

Sophie Le Pallec, Public Affairs Manager, GS1 France

François Lhemery, Public Affairs and Communication Deputy Director, Numeum

Smara Lungu, "Strategic Marketing, Competitive Intelligence and Ecosystems" Director, Docaposte

Julien Nocetti, Associate Researcher, IFRI

Marine Pouyat, Consultant, W Talents

Jean-Luc Sauron, Senior civil servant, Professor, PSL Université Paris-Dauphine

Anne-Claire Wang, Public Relations Manager, Huawei France

PROOFREADING

Jessica Galissaire, Studies Manager, Renaissance Numérique

Henri Isaac, Associate Professor, PSL Université Paris-Dauphine

We would also like to thank **Loane Bedouet** and **Pol-Euan Lacombe**, project assistants at Renaissance Numérique, who supported the working group throughout its discussions.

ABOUT RENAISSANCE NUMÉRIQUE

Renaissance Numérique is France's main independent think tank focusing on the challenges of the digital transformation of society. Bringing together universities, associations, corporations, start-ups, and schools, it aims to develop workable proposals to help public stakeholders, citizens and businesses build an inclusive e-society.

RENAISSANCE NUMÉRIQUE

32 rue Alexandre Dumas - 75011 Paris
www.renaissancenumerique.org

JANVIER 2022