

|                  |                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | Chapter 1-III : Leviathans in resistance and digital sovereignty : proposals for open innovation and governance                                                                                                   |
| Sub Title        |                                                                                                                                                                                                                   |
| Author           | Türk, Pauline                                                                                                                                                                                                     |
| Publisher        | Keio University Global Research Institute                                                                                                                                                                         |
| Publication year | 2025                                                                                                                                                                                                              |
| Jtitle           | Monsterizing Platform Power and Law ; Volume 1. Platforms and States: How to Settle the Battle of Monsters ,p.41- 54                                                                                              |
| JaLC DOI         | 10.14991/KO11003002.00000001-0041                                                                                                                                                                                 |
| Abstract         |                                                                                                                                                                                                                   |
| Notes            | Chapter 1 : Actors of the governance of digital space                                                                                                                                                             |
| Genre            | Book                                                                                                                                                                                                              |
| URL              | <a href="https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0041">https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0041</a> |

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

# LEVIATHANS IN RESISTANCE AND DIGITAL SOVEREIGNTY

: Proposals for open innovation and governance

Pauline Türk<sup>\*</sup>

---

## Introduction

States are confronted with new types of power: after media, international organizations and financial marketplaces, multinationals companies, mainly American, are acquiring sufficient economic clout to destabilize the political power of States<sup>1</sup>. This is the backdrop to the debate on digital sovereignty : the State appears to be threatened in the exercise of its functions by the emergence of competing powers<sup>2</sup>. Private operators – the digital platforms - have established themselves in a whole series of fields. Moreover, they have been able to strengthen their influence during the COVID-19 pandemic period.

## The rise of the concept of digital sovereignty

Reflection on digital sovereignty arises from a concern: the refusal to see peoples, communities of users, States and individuals lose control of their destiny to the benefit of ill-defined entities, which are not elected and cannot claim any other form of legitimacy, and whose objective is not the promotion of general interest.

The 2000s saw the first questions on the subject, and soon the very notion of “digital sovereignty”. On an international scale, the issue of control over internet resources has first crystallized the concerns of certain States, wishing to limit American hegemony over network management, particularly with regard to the strategic missions of ICANN (Internet Corporation for Assigned Names and Numbers), the Californian company created in 1998 whose strategic role is known in overseeing the management of domain names, strategic roots of the Internet. These concerns are all the more acute as the historical dominance of the United

---

\* **Pauline TÜRK:** Full Professor of Public Law, Director of the Centre for Study and Research in Administrative, Constitutional, Financial and Tax Law at Université Côte d’Azur ; President of the Scientific Board of the French Association for Constitutional Law, pauline.turk@univ-cotedazur.fr

1 Pauline Türk, « The sovereignty of States faced to the development of the Internet / La souveraineté des Etats à l’épreuve d’Internet », *Revue de droit public*, 2013, n° 6, pp. 1489-1521. <https://hal.univ-cotedazur.fr/hal-02493141>

2 Annie Blandin (dir.), *Digital rights and sovereignty in Europe / Droits et souveraineté numérique en Europe*, Bruylant, 2016, 216 p. ; Pauline Türk et Christian Vallar (dir.), *Digital sovereignty: the concept, the challenges/ La souveraineté numérique : le concept, les enjeux*, Mare& Martin, 2018, 239 p. ; Pierre Bellanger, *Digital sovereignty / La souveraineté numérique*, Stock, 2014, 264 p.

States is accompanied by a virtual technical and economic monopoly of American multinationals, in the field of operating systems and in the development of digital applications. The expression “digital sovereignty” was coined at the 2012 World Conference on International Telecommunications, notably by Russia and China. These States have demanded the restoration of their “sovereign rights” over network management, and the drafting of an international treaty for a greater sharing of responsibilities.

For their part, western countries were concerned, above all, to protect the freedom of cyberspace from state takeover attempts. Things changed in the wake of the Snowden affair, in 2013. Revelations of widespread espionage for the benefit of American political and economic interests have led to a profound rethinking of the system of governance of digital sphere governance, notably at several international summits and forums devoted to the subject (NETmundial in Sao Paulo in 2014, annual Internet Governance Forum in Bali in 2013, Mexico City in 2016, etc.). Following, in the footsteps of China, India and Russia, many other countries, such as Brazil, launched dedicated industrial programs and policies. 2013 also marked a “European awakening” on the subject, with the European Union (EU) taking an interest in the development of “sovereign” search engines or “sovereign” operating systems (OS), while renegotiating agreements with the United States on the protection of personal data of European users.

In France, meanwhile, the term “digital sovereignty” has gradually gained currency. As early as 2006, some specialists called for a rethink of state sovereignty because it is becoming inseparable from the tools of technological power<sup>3</sup>. The concept has been then popularized, and used by various government and regulatory bodies<sup>4</sup>. In 2014, the first Digital Sovereignty Conferences accompanied the creation of the French “Institute for Digital Sovereignty”, an association dedicated to the raising of awareness of these issues among public and elected representatives. The article 29 of the law “for a digital Republic” of October 7, 2016, enshrined the notion by proposing to create a “Commissariat à la souveraineté numérique” (finally abandoned), tasked with contributing “to the exercise, in cyberspace, of national sovereignty and individual and collective rights and freedoms protected by the Republic”. The debate has subsequently continued in Parliament, with the production of information and inquiry reports. Since then, digital sovereignty has usually referred to **the State’s ability to command and be obeyed in the digital world, to self-determine and defend its values and interests there, and to protect the rights of its citizens.**

At European Union level, also, digital sovereignty has become a major challenge for European institutions and political projects, after the new Cambridge Analytica scandal of 2018. The concept, here, is more political than legal, since the European Union is not a sovereign state. The issue is rather in the risk to the European union resulting from its technological dependence. In 2020, the President of the European Commission announced a vast plan to reconquer European digital sovereignty by 2030. And the European Council set the course: concrete objectives (digital education, consolidation of infrastructure, digital transformation of companies, digitalisation of public services) are pursued by the “Digital Compass”, presented in March

3 Bernard Benhamou et Franck Sorbier, « Sovereignty and digital networks / Souveraineté et réseaux numériques », *Politique étrangère*, 2006/3 Géopolitique de l’Internet, p. 519 à 530.

4 Pauline Türk, « Digital sovereignty: challenges and definitions / La souveraineté numérique : enjeux et définitions », *Cahiers Français*, Doc. Fr. mai 2020, n°415, pp. 18-28. HAL : <https://hal.science/hal-02493091>

2021, supplemented in 2022 by a European declaration on the rights and principles of digital education. Concerns about digital sovereignty, now, take on three major dimensions: the protection of personal data and the fundamental rights of European citizens; economic and industrial strategy issues; and geopolitical and governance issues. These concerns are reflected in an avalanche of working documents, political speeches, measures taken by the European legislator and rulings by the Court of Justice of the European Union<sup>5</sup>. And numerous regulations have been adopted to promote the European conception of technological development ((General Data Protection Regulation (2018), Digital Market Act and Digital Services Act (2022), Data governance Act (2022), Data Act (2024), Artificial Intelligence Act (2024)), contributing to the “Brussels effect”<sup>6</sup>.

### **The state facing digital giants: competition, collaboration and imitation**

Professor Yamamoto has proposed an original reading of the existing relationship between states and multinational companies concerning these questions of new power relationships, i.e. especially American digital platforms. His perspective is confronting two monster species, Leviathan States on the one hand, and “Digital Giant Behemoths”, representing the multinational companies, on the other. Establishing a parallel with the relationship between the temporal power of the State and the spiritual power of the Church is a new way of explaining the relationship between these two types of monster. Several models for organizing the relationship between state and church have been identified: State religion, concordat (i.e. an intermediary mode based on collaboration), strict separation between secular and religious powers. In the same way that the Church and the State could, depending on the case, be separated or partners, the Leviathan States and the Behemoths could, depending on the continent and the culture, collaborate or oppose each other, according to three models presented by Professor Yamamoto. He notes that Europe is leaning towards “digital secularism” - relatively strict separation system-which is confirmed by our attachment to the concept of digital sovereignty.

As we know, Europe has adopted an approach oriented towards the defense of the sovereign State. The authority of public power is crucial in the work of Jean Bodin in France, of Jellinek in Germany, and of Machiavelli in Italy, etc. State sovereignty has been at the center of the organization of the European continent since the Treaty of Westphalia, 1648. European relations have been organized around confrontation and thereafter collaboration between the European nation-states. While the Leviathan States have -finally- figured out how to maintain peace between themselves, the Behemoths have destabilized this organization of powers.

In France in particular, the State has fought to affirm the autonomy of the temporal power of the State over the religious spiritual power, with the aim of confining each one within its sphere of power, by inventing the concept of “Laïcité”. Firstly, France is very attached to the concept of State sovereignty and defends it against

5 Pauline Türk, « European Digital Sovereignty: Towards a Third Way? / La souveraineté numérique européenne, vers une troisième voie ? », *Pouvoirs, La souveraineté européenne*, n° 190, 2024, pp.79-90 ; B. Bertrand et G Le Foch, (dir.) *Digital sovereignty / La souveraineté numérique*, Bruylant, 2024, pp. 65-81 ; Danet (D), Desforges (A), « Digital sovereignty and strategic autonomy in Europe: from concept to geopolitical reality », (*Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques*), *Hérodote* 2020/2-3, n° 177-178), pp. 179-195.

6 Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, 2019, Oxford University Press.

new competing powers. Secondly, France's positioning can also be explained by its attachment to the welfare state and to public services. The public sector is called upon to take charge of the services most necessary for citizens, while the private sector provides complementary services. Thirdly, this particular sensitivity can also be explained by French attachment to human rights, which has been defended by the State since 1789.

Finally, competition from the "Behemoths" is cause for concern because it threatens the ability of the State to guarantee fundamental freedoms, public services, and respect for democracy. Only the State is in charge of promoting the general interest, unlike multinational companies that pursue their private interests or those of foreign states. This has been made even more obvious after the Snowden and Cambridge Analytica affairs, when Europe has become aware of the surveillance exercised over citizens and their governments by the giant platforms. As observed by Shoshana Zuboff, "Liberal democracies have failed to construct their own coherent vision of a technological future that promotes democratic forms of government", in a context of "surveillance capitalism", involving a new type of power seeking to monitor, target, analyze, manipulate and control individuals, groups, and populations<sup>7</sup>.

Faced with these new challenges, my purpose, here, is to consider how the perception in Europe and in France about the relationship between States and platforms has been evolving. Alongside the approach of separation, confrontation, and competition, another perception has been developing, that is more open to collaboration and partnership. And that is for pragmatic reasons.

I would first like to emphasize the competitive nature of relations between states and platforms. It is true that the discourse on digital sovereignty presents the vision of a State that is "caught up by", that "competes with", and is sometimes "overtaken" by other players. This vision challenges the action of public authorities and the future of "State model". As Zygmunt Bauman observes, the state is no longer the only operator in *"economics, security, or culture, and it can no longer promise its subjects full protection, from cradle to grave, that it was trying until recently to provide"*. As a result, *"the once complete and integral sovereignty of the nation-state is evaporating into the anonymous realm of global forces escaping territorial allegiances and commitments"*<sup>8</sup>. Consequently, States seek to reassert their authority in the logic of confrontation with platforms (Part I).

Secondly, I would like to highlight the emergence of a new, more collaborative dimension in the relationship between state and digital powers, in search of a form of complementarity. With pragmatism, European countries are on the road to accepting a necessary redistribution of roles between the State and private digital operators. The rise of platforms is forcing States to seek dialogue. This may lead to a redefinition of the scope and nature of services expected from public authorities. This is reflected in certain forms of collaboration, where States are now cooperating with private digital operators and outsourcing some of these activities to them. The Digital Services Act of 2022<sup>9</sup>, for instance, highlights an evolution in the relationship of European

7 Surveillance capitalism is defined as a new form of market that harnesses data from human experience, appearing as a free raw material to be translated into behavioral data for use in covert operations of extraction, production and sale. Zuboff (S), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, NY, PublicAffairs, 2019.

8 Z. Bauman, *Liquid life/La vie liquide*, Fayard/Pluriel, 2006, p. 75.

9 Regulation (EU) 2022/2065 of the European Parliament and of the council of 19 October 2022 on a Single Market For Digital

States to platforms, considered as mandatory partners in the regulation of freedom of expression online. This paradigm shift is also reflected in the logic of mimicry, which can be described as the “platformization of the State”. In France, the government has undertaken to transform the State to make it “think of itself as a platform”, by adopting the codes of the collaborative economy based “on new value creation processes to offer better quality services to citizens”. This is another signal of ‘*rapprochement*’ between State and platforms (Part II).

## 1 STATES IN COMPETITION WITH NEW POWERS IN THE DIGITAL WORLD

The State has been weakened and is now in competition with new digital giants in its two essential roles: exercising of public authority and providing public services.

### A States compete for the power to command and to be obeyed

First of all, the mission of the State is to exercise authority as a public power that both constrains and protects. This includes the drafting of laws, their application and sanctions for their violation. Sovereign functions, police, military defense, taxation or justice, are of course mainly involved. Platforms interfering in the exercise of these prerogatives confiscate part of the State’s sovereignty.

#### 1) States are therefore faced with a weakening of the attributes of their authority.

Because of the rise of digital networks and platforms, public power is weakened and challenged, and is now struggling to enforce its tax policy, its political choices, or its laws in the digital world<sup>10</sup>. In the early days of the digital revolution, States may have had to adapt whole sections of their legislation that had become inapplicable. For example, in the case of France, legislation on online gambling and on the publication of polls during election periods had to be overhauled because they had become unworkable. Some States are struggling to apply regulations that require regular adjustments, for example for protecting privacy policy, human dignity and interests of minors. Protecting the foundations of democracy and the sincerity of elections has become a concern, forcing legislators to rethink the fight against fake news, an old concern that is now taking on a whole new dimension<sup>11</sup>. A whole underground economy escapes the law, notably on the deepnet and the darkweb, which are precisely designed to allow online browsing outside the radar of public authorities. State

Services and amending Directive 2000/31/EC (Digital Services Act).

10 Céline Castets-Renard, Valère Ndior, Lukas Rass-Masson, *International challenges of digital activities: between the territorial logics of States and the power of private actors / Enjeux internationaux des activités numériques : entre logiques territoriales des Etats et puissance des acteurs privés*, Larcier, 2020, [202 p. ; Eric Sadin, *La siliconisation du monde : l'irrésistible expansion du libéralisme numérique*, 2016, L'échappée ; Bruno Jobert, et Jacques Commaille, *Les métamorphoses de la régulation politique*, 2019, LGDJ, Droit & Société ; Eric Schmidt, Jared Cohen, *The new digital age : Reshaping the Future of People, Nations and Business*, Hachette UK, 2013.

11 See the new means of fighting anti-fake news in the 2018 French law (LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information) and the 2017 “NetzDG” German law (Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352).

is facing difficulties in enforcing laws on transnational and dematerialized networks (security and public order, commercial law, copyright, right to the protection of personal data, confidentiality of health data, etc.). Offenders take on many faces and are sometimes heavily armed technically and legally: State spies, malicious hackers, secret services at work, commercially interested companies, variously inspired users, etc.

It is also increasingly difficult for States to enforce certain political choices or certain decisions made by public authorities on their own territory. Court decisions can be criticized on transnational digital networks. The separatist aims of certain provinces can be encouraged. The decisions of political leaders can be discussed. The institutional practices or official speeches can be criticized, discredited or distorted. Moreover, the weight of misinformation and the risk of opinion manipulation are rising dangerously. Despite a gradual takeover of networks by the States, their authority has been undermined. States remain powerless against the disclosure of sensitive documents, regularly reported in the media, sometimes even in the case of highly classified documents. The judicial system, for its part, is struggling to maintain the secrecy of investigations, and sometimes sees the effect of its decisions limited<sup>12</sup>.

## 2) The rise of a new kind of political and economic power

At the same time, States are facing the rising power of new standard-setting and decision-making leaders. Major private and transnational digital operators have normative powers because they master “the code”<sup>13</sup>. We all know that digital giants exercise power over a territory (non-physical and transnational) and over a population (physical and connected Internet users). These new actors, whose economic and financial power is equivalent to that of certain States, have the power to set rules, standards, norms and conditions of use. Users are forced to accept these rules, because they depend on the technologies. Platforms have also adopted certain attributes of sovereignty: virtual currencies, police (control, withdrawal of content), justice (dispute settlement), and normative power (setting of the General conditions of use /Terms of use). Actually, globalization of economy and law had already led to the emergence of new modes of regulation, in the hands of transnational organizations, groups of experts and private operators. After *lex mercatoria* and *lex sportiva*, *lex electronica* covers all the rules resulting from the self-regulation of actors in cyberspace<sup>14</sup>. The paradigm of the hierarchical and unilateral power of the State towards its citizens is cracking<sup>15</sup>. New powers compete with its authority. States are contested in their ability to command and be obeyed by multinational companies that enjoy supremacy because of their dominant position on the market. For instance, States face difficulties in applying their tax policies to multinationals whose subsidiaries are organized to circumvent them. They are also fighting against virtual currencies that escape State regulation<sup>16</sup>. In the same vein, the creation of

12 In 1996, for instance, the Tribunal de Grande Instance de Paris prohibited the distribution of a book written by the private doctor of the former french President François Mitterrand, doctor who had been convicted of violating privacy and professional secrecy. While paper copies of the book may have been banned, the distribution of its contents on the Internet could not be prevented.

13 Laurence Lessig, *Code and Other Laws of Cyberspace*, Basic Book, 1999.

14 P. Trudel, F Fabran, K Benyekhlef et S Hein, *Cyberspace law / Droit du cyberspace*, Montréal, Themis, 1997, p. 15.

15 François Ost et Michel Van de Kerchove, *From the pyramid to the network? For a dialectical theory of law / De la pyramide au réseau ? Pour une théorie dialectique du droit*, Presses de l'Université Saint-Louis Bruxelles, 2010.

16 A. Laurent et V. Monvoisin, « New Digital Currencies: Beyond Monetary Dematerialisation and the Contestation of Banks », *Revue de la régulation : Capitalisme, institutions, pouvoirs*, 2015, n° 18, p. 1-24, <https://doi.org/10.4000/regulation.11524>

dispute settlement bodies or quasi-judicial bodies by platforms is another sign of the way platforms are assaulting State sovereign functions. A typical example is Meta's oversight board (Facebook's supervisory board), responsible for rendering "independent judgments" and regulating freedom of expression, power that is exercised over a community of 2 billion people.

Another problem is that citizens' sense of belonging to a state community may be undermined. Digital world is a place where transnational groups can come together, developing new forms of belonging, not determined by physical borders of States. Some are already anticipating the construction of immaterial political societies, "*virtual states, which will disrupt the landscape of physical states*"<sup>17</sup>. Some of these plans are materializing in the projects of Metaverse. Finally, new forms of citizen participation, including direct democratic tools, can undermine our representative systems. Some political parties no longer hesitate to imagine new forms of government (for instance European pirate parties that are now represented in the European parliament), casting doubt on the usefulness of state's government institutions.

Private sector and user's societies are associated in the development of new forms of normativity and new regulatory mechanisms. States, and the international organizations they create, no longer have the monopoly in drafting rules. In the exercise of their mission of authority and protection of citizens, States are therefore weakened and in competition.

## B The State competes in providing services to citizens

The second main function of States is to provide diversified services to their citizens.

### 1) Public services in competition with more efficient services provided by platforms

The exercise of a State's competencies is now conditioned, in various fields, by its dependence on digital networks and those who govern them. For instance, in the field of transport services, "hire car with driver" sector (Uber or Blablacar platforms) has challenged the monopoly of taxis, which is, in France, a state-regulated profession. In the same direction, the French public employment service (France Travail, formerly Pôle Emploi) is competing in providing assistance to job seekers with professional social networks and platforms (LinkedIn, Monster, Indeed or Viadeo). As a third example, concerning road traffic, the former national information and security service, entrusted to the Ministry for Ecological Transition, has been replaced by collaborative applications for driving navigation assistance using mapping tools and geolocation (WAZE, GoogleMaps or the French MAPPY). Finally, the National Road Information Center created in 1968 was dissolved in 2016 and the French service "Bison Futé", "*emblem of the public road information service*", gave way to efficient mobile applications offered by private operators.

More generally, state's- traditional- modes of intervention have been challenged and destabilized by the development of the collaborative model proposed by platforms. In France, in 2020, during the pandemic, the public service of higher education was faced with the need to offer an efficient online alternative to face-to-face courses. It had to adapt its programs during a limited time. In most cases, the services offered by private

<sup>17</sup> Eric Schmidt, Jared Cohen, *The new digital age*, Denöel, 2013, p. 15.

platforms were used to provide distance learning, in preference to the less efficient services set up by the Ministry of National Education. Similarly, in the health sector, management of medical appointments for the anti-covid 19 vaccination campaign could not be ensured by the State alone. Private operators were called on, such as the Franco-German company “Doctolib”. Health data protection guaranteed by this company, which hosts some of its services on the Cloud of Amazon Web Services (AWS), have given rise to criticism and litigation.

Public services linked with cultural information and dissemination are also challenged by the emergence of private digital operators, such as social networks (Twitter, YouTube or Facebook) or streaming services (Netflix, Spotify, Deezer). Even the archiving of public documents is concerned: public authorities have had to resort to the more efficient cloud services offered by private operators, even if they were finally asked to return to “sovereign” solutions<sup>18</sup>. Many sectors of public action must adapt to this form of competition.

## 2) The consequences for the welfare state model

In France, particularly, the welfare state is a provider of public services “*necessary for social interdependence*”<sup>19</sup>. However, some people fear that new and efficient services offered by digital platforms will mark the decline of the welfare state, and the advent of a neoliberal model. This could create an unbalance in social and political order in favor of economy. It could also destabilize our democracies. In its 2017 annual study, the French Council of State noted “*the disruptive consequences for the public service of the emergence of digital platforms which compete directly with it*”. It also noted that “*the economic model of the digital platform can lead to the spontaneous take over, by private initiative, of activities regarded as falling within the nature of the public service*”, and that it moreover allows “*activities to be profitable which, until then, were not economically profitable*”<sup>20</sup>. It is indeed a crisis of the welfare state when the private sector takes over certain types of services and thereafter provides a better offer than the one of public authorities. In the end, citizens could no longer expect the State to provide the services they need, which can thus reduce their dependence on the State framework and its administration.

However, services rendered by the State are the counterpart of obedience to the law and the payment of taxes. Loss of these services can weaken the social pact. Individuals may be tempted to “*regain their rights in the presence of a minimal state*” when “*the welfare state and its corollary – taxation – are considered abusive*”. Users may be led to choose, on a case-by-case basis, which collaborative community they want to belong to, and the role they want to play in it, depending on the services they need, in exchange for agreed duties and obligations (acceptance of CGU or use of their data for example). Thus, with increasing competition from the private sector for exercising different types of mission, including those relating to its sovereign functions, States must adapt the services they provides to make them as effective as those offered by online

18 An inter-ministerial memo of April 5, 2016, addressed to Prefects and local authorities, reiterated the obligation, under penalty of illegality, to choose a “sovereign cloud” solution. A new memo from the Inter-ministerial Digital Department (DINUM) in 2021 reaffirmed the formal ban on the use of non-sovereign clouds for the collaborative work of public officials.

19 Léon Duguit, *Traité de droit constitutionnel*, Tome 2, 1928.

20 French Conseil d’Etat, *Public power and digital platforms: accompanying uberization*, annual study, 2017, <https://www.conseil-etat.fr/publications-colloques/etudes/puissance-publique-et-plateformes-numeriques-accompagner-l-uberisation>

collaborative platforms, if they want to preserve the foundations of their authority. Failing this, they will have to develop other ways of making themselves essential for the functioning of citizen communities.

## 2 REDEFINING THE ROLE OF THE STATE, LOOKING FOR COMPLEMENTARITY

Platform and private digital operators interference or competition can lead the State adapting its service offer and redefining its scope or management methods. Some public services are doomed to disappear. But others have been created such as, in France, the new “public data service” created by the law for a Digital Republic in 2016<sup>21</sup>. Far from being erased, the State’s role is changing. The State is acting more like a facilitator, a sponsor, an organizer, or promoter of the construction of new efficient services. We notice two developments : one involves collaboration with digital companies, in a logic of complementarity (A). The other corresponds to a process of imitation that allows the State to adopt the platforms’ recipes for success (B).

### A Public authorities outsource to digital private operators

Subcontracting certain tasks to digital operators can be illustrated, for example in the field of regulation of online content and the health sector.

#### 1) The need for a partnership with platforms to exercise effective regulation of illegal content

For a long time, Member States of the European Union thought they could regulate freedom of expression online themselves and did not want to entrust this role to the platforms. This is how France enforced its traditional legislation on freedom of expression, adapted it, and applied a limited liability regime to platforms<sup>22</sup>. In accordance with article 14 of European Directive 2000/31 of June 8, 2000, on electronic commerce (e-commerce), a system of exemption from liability has been organized for platforms, considered as simple intermediaries in the case of illegal hosted content.

But since then, States have gradually become aware of the need for a partnership with platforms to exercise effective regulation of illegal contents. Collaboration was first imposed on platforms asked to fight against certain particularly serious offences. In France, laws aimed at combating online hate and disinformation need the platforms to cooperate. For instance, the “anti-fake news” law of December 22, 2018, requires online platform operators, depending on their size, to contribute regulating fake news during the election period. Germany, too, passed a law to fight illegal online content in 2017 (‘NetzDG’ or Network Enforcement Act of October 1, 2017) that requires platforms to remove hateful content. For efficiency reasons, the 27 European Union Member States can no longer expect to regulate online expression each in their own way, without the platforms help. Collaboration with them appears necessary for a homogeneous and effective reg-

21 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

22 Pauline Türk, « Liberté d’expression et désinformation en France. Entre tradition libérale et impératif de régulation : un encadrement souple de l’expression en ligne », in O Pollicino (dir), *Freedom of Speech and the Regulation of Fake News*, Cambridge, Intersentia, 2023.

ulation of online content. That is what the new *Digital services Act* of October 19, 2022<sup>23</sup>, covers, empowering the platforms to regulate and makes them State partners. Platforms, depending on their size, are required to cooperate in different ways with the national authorities: by appointing ‘*referents*’ and setting up effective reporting tools, by ensuring the transparency of their algorithms, by carrying out analyses and audits of the risks generated by their activity, and by taking preventive measures to protect minors specifically. A kind of partnership is emerging, even if it is based on constraint: the European Commission can impose sanctions in the case of the non-collaboration of its relevant private operators.

## 2) The need for platforms high-performance technological solutions in the healthcare sector.

In some areas, the French State has tried to develop these technological solutions itself. The Ministry of higher education, research and innovation set up the platform for access to higher education (*Parcoursup platform*). In police matters, government services have developed, with their own means, software for preventing the theft of police cars (*predvol*).

But the State must, in some cases, use private operators services for all or part of the technological solutions they need (for reasons of cost, schedule, or level of technicality and performance, etc.). Particularly in the field of health in France, it has been observed when creating and setting up: national health data system or the Health Data Hub; *StopCovid/TousAntiCovid* tracing applications; or even the management of appointments for the vaccination campaign in the urgent context of the COVID-19 pandemic. The French State relied on the private operator’s services to develop the French health data platform (or *Health Data Hub*) in 2019. This was the subject of debate because of the public authorities’ decision to use Microsoft services, and more specifically its AZURE cloud computing service. This platform consists of a public interest group and a national health data system that allows the collection, storage, sharing and use of health data, and also serves to inform patients and promote their rights<sup>24</sup>.

French choice, in 2019, was based on pragmatic considerations, because, as the public authorities have acknowledged, there was, at the time, no “sovereign” solution that met all the criteria of quality and efficiency. The Health Data Platform therefore signed a contract, on April 15, 2020, with the Irish company Microsoft Ireland Operations Limited, a subsidiary of the American company Microsoft Corporation. This contract has set the conditions of using “Microsoft Azure” products, including the hosting of health data and the granting of software licenses necessary for the processing of data for legally authorized purposes.

However, the French National Agency for regulation of Data Protection (Commission nationale informatique et liberté) stressed that the sensitivity of health data was justifying a high level of technical and legal protection. Data being captured by countries outside the European Union has been a main concern. Under a judicial appeal, the Council of State allowed Microsoft’s adherence to the Privacy shield of 2016<sup>25</sup> as a suffi-

23 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC/.

24 Articles L1462-1 and L. 1461-1 of the Public Health Code.

25 Privacy Shield, a data protection framework that was designed to allow for the transfer of personal data between the EU and the United States, was created as a replacement for the previous Safe Harbor framework, which was deemed inadequate by the European Court of Justice in 2015 (Schrems I).

cient guarantee. As we know, the Privacy Shield was later invalidated for being inconsistent with European requirements by the Court of Justice of the European Union<sup>26</sup>. As a result, trust placed in the services of the American company Microsoft Azure was seriously undermined; especially with regard to the risk that the personal data of European citizens might be transferred to the United States. And, also, because of a lack of adequate judicial remedies to protect against this risk, due to the extraterritorial application of American law and to the prerogatives of American public authorities<sup>27</sup>. The administrative judge (French Council of State) pointed out the risk of data transfer and requested additional guarantees but did not invalidate this partnership with Microsoft given the pandemic<sup>28</sup>. However, it advised the State to quickly choose a new subcontractor, as soon as technically possible. The requirement of “digital sovereignty” has led the government to look for other providers, who are still private operators, but are European companies. However, the need for a partnership with digital companies still remains.

For a second example, France refused the technological solution proposed by Apple and Google called “Exposure notification” when it came to implementing contact tracing solutions to fight against covid. France immediately moved towards a “sovereign” solution (“StopCovid” and afterwards “TousAntiCovid”(TAC) applications). The French public and private partners (INRIA, ANSSI, Dassault, Capgemini, etc.) were called on to keep data on the national territory. Data storage has been ensured on a French company server (3DS/Outscale - Dassault), accredited by ANSSI, under the responsibility of the General Directorate of Health. However, the “TAC verif” application did require, for some stages of development, the use of APIs provided by subsidiaries of the American giants, such as Akamai (a service provider of IN Group, the national printing company) and Google.

As a third example, the management by the State of the COVID-19 vaccination campaign involved collaboration with private digital operators, including several start-ups (Keldoc, Maiia and, mainly, the Franco-German company Doctolib). As already noted, the latter relied on the technical solutions of Amazon Web Service (AWS). AWS is a European subsidiary of the American company Amazon, subject to the same legal constraints as Microsoft, under American extraterritorial application laws. It gave rise to a new litigation before the administrative judge (Council of State). It has not been considered evident that “the decision of the Minister of Solidarity and Health to entrust the company Doctolib, with the management of appointments for vaccination against COVID-19, constitutes an illegal violation of the right to respect for private life and the right to the protection of personal data”<sup>29</sup>.

Thus, the field of public health shows new kinds of partnerships between the public authorities and private digital companies, including platform operators. Digital companies are the only ones capable of offering the technological solutions needed for the development of new services. The logic of competition has been transformed here in a search for complementarity between the State and the most efficient private digital

26 Privacy Shield was invalidated by the European Court of Justice on 16 July 2020 (Schrems II case).

27 Within the framework of programs of surveillance based on the Foreign Intelligence Surveillance Act (FISA) and Executive Order (EO) 12333).

28 French Conseil d’Etat, 13 octobre 2020, n° 444937, Health Data Hub.

29 French Conseil d’Etat 12 mars 2021 n° 450163, Interhop.

operators. But concerns about digital sovereignty remain, leading to a preference for European solutions wherever possible. Data protection policy has led the French State to search for ways to cooperate with European digital operators and platforms, rather than with the major American platforms and their subsidiaries.

## B Public authorities imitate the platformization of public services

States may be in competition with the major platforms in the exercise of their missions, but it may also seek new forms of complementarity with the private sector. Transforming the conditions for exercising those services they will continue to provide will be necessary, as well as redefining the scope of these services.

### 1) Platform State's ambitions

In 2017, the French council of state's annual study entitled "*Public power and digital platforms: supporting uberization*", raised the question of the evolving "scope of public services". It suggested "to challenge the relevance of maintaining them" and to "redesign the map", with this aim of directly considering services which could be better provided by private platforms could disappear or be adapted. It does not mean a disengagement of the State, but that the State needs to identify the missions which remain its core business. It has to determine which public services need to be strengthened and which need to be created (for instance a new public data service mentioned above, or the new public service for digital education founded by the law of July 8, 2013 on the refoundation of the French school system.). As early as 2012, Nicolas Colin and Henri Verdier called on the French state to adapt to the innovation economy and draw inspiration from the way platforms are operating. The French State was called on to adopt the recipes for the platforms' success. Considering that "the administration must guarantee the best quality of service to its citizens", even though it might be "difficult for the administration to reach the level of excellence of the services offered by the digital economy", it is for public authorities an "objective and a duty"<sup>30</sup>. This approach is explicitly inspired by Tim O'Reilly's book, who has proposed the concept of "platform state", defined as a "bazaar" where you can find all the material useful for building the services you need. It means rethinking public action methods "*If instead of seeing it as a vending machine, we imagine the administration as the manager of a market place?*"<sup>31</sup>. It also means transposing the platform specific collaborative operation to States, valuing the creativity of the multitude. Public authorities would no longer be offering users the service itself, but the infrastructures and resources needed to co-construct it.

Thus, States must redefine their missions in the digital age and have no choice but to adapt the way of exercising them, to remain efficient and competitive. Among European States, Estonia, Denmark, the United Kingdom and Spain stand out in this field. In France, public strategy is based on an open data policy supported by the inter-ministerial digital department (DINUM) and by the Etalab mission. We are still at the beginning of a transformation process<sup>32</sup>. It has been observed that France is struggling to digitize its public

30 Nicolas Colin et Henri Verdier, *The age of the Multitude: Entrepreneurship and Governing after the Digital Revolution / L'âge de la multitude : Entreprendre et gouverner après la révolution numérique*, 2012, Armand Colin.

31 Tim O'Reilly, «Government as a Platform », *Innovations : Technology, Governance, Globalization*, vol. 6, n° 1, 2011.

32 Pauline Türk, «The State as a digital platform/ L'État plateforme numérique », *Revue du droit public*, n°5, p. 1189.

policies: “security, education or the deployment of energy infrastructures still seem to be considered at best as if digital technologies were a simple commodity, at worst as if they did not exist”<sup>33</sup>. In its 2018 annual report, entitled “Amplifying the digital modernization of the State”, the French Court of Auditors (Cou des comptes) set out the results and the limits of this strategy and recommended that the French State invest more in order to “move into the next century” and carry out “the deployment of the platform state strategy”<sup>34</sup>. After the creation of an open license in 2011 and the development of the data.gouv.fr platform, dozens of services have been tested in recent years.

## 2) Towards a transformation of the state

Some are wondering if those evolutions will lead to “a new avatar of neo-liberal state reform”<sup>35</sup>. All this policy would conceal a technocratic project to challenge the welfare state, based essentially on considerations of profitability. But admittedly, the project consists in letting the citizens solve the problems that they can solve themselves, helping them and promoting their initiatives. And certainly, some imagine public services without administration, self-organized by communities of citizens, contributing and interacting, becoming co-producers of the service they use, to the detriment of the national state authorities.

But rather than a weakening and a disengagement of the State, this project can also give a glimpse of its possible transformation and even its strengthening. In the future, the State can concentrate on the services attached to its sovereign functions. Or it can take over unprofitable services leaving the rest to the private sector. Or it can strive to better perform the missions for which its intervention is necessary or preferable. Or, finally, it can take on new missions of encouragement, support, promotion and regulation of private initiatives in the co-construction of services.

---

## Conclusion

To use Professor Yamamoto’s metaphor, Leviathan states are seeking both to defend their authority against the Behemoths, while exploring, in certain areas, a form of cooperation. Certain ways of collaboration are appearing in certain fields. In other areas, Leviathan States are copying how digital platforms work. They are somehow transforming into platforms, to be more efficient, and to stay competitive in the provision of services, faced by the “Behemots”.

Around the world, sovereign states are exploring different ways to coexist and cohabit with new powers, in search of new balances. Enforcing their laws, protecting their citizens, adapting the scope of public services and modernizing the way they are provided, developing an industrial strategy limiting dependence on (American) multinationals, are among their main objectives.

In any case, for the time being, the State remains the reference framework for human communities. And

---

33 French Cour des comptes, « Amplifier la modernisation numérique de l’Etat », Rapport public annuel 2018.

34 Idem.

35 « IA et réforme de l’Etat : vers des bureaucraties sans humains ? », La Quadrature du Net, janvier 2022, <https://www.laquadrature.net/2022/02/18/ia-et-reforme-de-letat-vers-des-bureaucraties-sans-humains/>

in a democracy, the reaffirmed authority of States still remains a guarantee for the protection of citizens' rights and interests. The question of digital sovereignty is linked to the State's ability to protect its citizens. Digital sovereignty is therefore not only a legal issue, but also a political, economic, strategic and industrial one.