Digital sovereignty: ten years of debate, and afterwards?

THE MULTIPLE FINDINGS OF INADEQUATE DIGITAL SOVEREIGNTY

The debate on digital sovereignty, a topic that divides digital and institutional actors, coincides with the arrival of the commercial Internet in the early 1990s. The combination of the deindustrialisation of our telecom industries, the de-digitalization of our state computing and a growth model based on the use of services from major US platforms has put us in a highly dependent position. With the war in Ukraine, France must now ensure that it still has some form of digital resilience by relying on its local ecosystem.

A critical discourse unfolds on the orientations taken by France and the European Union in the field of digital sovereignty. It focuses partly on the place of law. It would confine the Union to a subordinate role when others (the United States in the first place) master the foundations of digital. To shed light on this issue, the article presents digital sovereignty as a fact and by law. The fact situation is that large platforms are propelling themselves into the field of sovereignty. To catch up, the European Union relies on competitive regulation while at the same time working to lay the foundations of an ethics through sovereignty.

The Covid pandemic has reinforced pre-existing trends: technological interdependencies that are still real, but thwarted by competition between the United States and China, and the problem of diversifying value chains. The war in Ukraine, which began in February 2022, has only accelerated a global movement towards the consideration of sovereign logics in the digital field. States are naturally acting in different ways depending on their political regime, giving rise to responses and counter-responses combining legal, financial and technological tools. Used for (geo) political ends, digital sovereignty is therefore more than just an industrial ambition – a trend that is likely to be reinforced by the superposition of international crises.

24 **The uncertain future of transatlantic data flows**
Florence G'SELL

The legality of data transfers between the European Union and the United States has been a long-standing issue, given the very different approaches to personal data protection on both sides of the Atlantic. The agreements that aimed to regulate and legalize transatlantic data flows – Safe Harbor, and then Privacy Shield – were successively invalidated. The new mechanism in place, the recent Data Privacy Framework, is already being contested, which casts a real uncertainty on the possibility for companies to effectively transfer data to the United States.

30 **Digital confidence or autonomy, the choice is yours**
Jean-Paul SMETS

The digital trust, the exorbitant role of the *Agence nationale de sécurité des systèmes d'information* and European regulatory inflation are creating unfavourable market conditions for many European digital technologies and open source software. Together, they are accelerating the adoption in France of American cloud technologies that are not immune to unauthorised access by a third country. They are increasing the risk of blackouts by favouring centralised cloud offerings that are not very resilient. When it comes to cyber risk management, the concept of "transparency" offers an alternative to "trust" to strengthen European industrial autonomy in digital on a technologically resilient and immune basis to unauthorised access by a third country.

39 **China's AI policy: how China is playing Go**
Paul JOLIE

China's current leaders intend to see the country return to world leadership, ahead of the United States, by 2049, the centenary of the CCP's arrival in power. This includes a predominance in key technologies, including AI, for both civil and military purposes, as well as for geostrategic influence.

The roots of this strategy go back a long way (political: Deng Xiao Ping's speech in favour of science and technology in 1978, then Xi Jinping's vision of a digital China; scientific, with pioneering Chinese mathematicians and impatriate Chinese scientists). It is supported by planning that intensified for AI from 2016, amplified by the 13th and 14th plans. The plan calls for China's basic AI industries to exceed RMB 1,000 billion by 2030, and for the country's AI-related industries to exceed RMB 10 trillion. A range of measures are being taken to achieve this ($4.7 billion in R&D for AI, private-public links, patents, brain drain, dedicated funds to buy start-ups outside China, public procurement, large-scale use of data made possible by the population).

THE STRONG LINKS IN DIGITAL SOVEREIGNTY

54 **The IMT at the heart of the national strategy
for digital sovereignty**
Francis JUTAND

Sovereignty has lost its nationalistic connotation to emerge as a necessity on the French and European agenda. It is a search for autonomy through the ability to choose through the mastery of key sciences and technologies, the ability to build complex digital systems, and by being a player in the writing of global rules that

organise competition, security and the use of soft power. France's industrial sovereignty has been undermined by globalisation, with digital European sovereignty short after the dynamics of global oligopolies GAMAM and BAIDU.

The IMT is at the nodal point of sovereignty, it trains the design, engineering and management frameworks to carry the digital transformation of the economy and society and produces knowledge on technologies, architectures, security, uses and transformation of companies. IMT is a source of innovation through the support of companies and the incubation of start-ups.

61 Europe: digital sovereignty and the challenge of technological autonomy
Henri d'AGRAIN

The concept of sovereignty, particularly in the digital field, is being used more and more in the public space. However, it is often misused, and in a way that does little to enlighten the debate on the risks that our loss of technological autonomy poses for the European continent and its economy. In the first part of this article, we attempt to shed some light on the concept of digital sovereignty. In the second part, we present the main risks that Europe faces as a result of its technological dependence.

66 Regaining the levers of sovereignty in cyberspace through a better organisation of missions in the field of cyber security
Hugo ZYLBERBERG

In a cyber environment that is now characterised by digital instability, it is essential to find ways of taking better account of cyber risk at all levels of organisations. To this end, the way the State is organised seems to be a useful way of identifying priority functions and strategic objectives that provide a practical response to these major cyber security challenges.

70 Can we move towards quantum sovereignty?
Alice PANNIER

Quantum information science and technology is a vast field that includes computing, telecommunications, detection and sensors, with a wide range of applications. Taken together, these technologies promise to revolutionise our information systems. The significant advances in quantum technologies in recent years, and their implications for security and the economy in particular, have created a real momentum of interest among governments, including in Europe.

Despite the impressive advances made by the two giants, China and the United States, and unlike most other digital technologies, Europe (in the geographical sense) is well placed in the global race for quantum technologies. On this promising basis, can Europe hope to achieve technological sovereignty in quantum technology? There are two main challenges: firstly, reconciling the objective of sovereignty with international cooperation, and secondly, ensuring that any quantum strategy is rooted in a holistic, long-term perspective.

75 Sovereignty and digital resilience: impossible mission?
Olivier BEAUREPAIRE, Thomas BOLLE, Sophie LAFON & Stanislas SMIEJAN

This article summarises the thoughts of the mission carried out for the *Fondation Nationale Entreprise et Performance* on the general theme of digital sovereignty.

The authors have focused on two specific subjects, quantum computing and the ethics of artificial intelligence, two areas in which the members of the mission believe that France and Europe can maintain their sovereignty, and show, in their recommendations, how this can be achieved and the pitfalls to be avoided.

81   Does our digital life depend on undersea cables?
Ophélie COELHO

The first submarine telegraph cables in the 19th century were already a strategic power issue exploited by states. Today, maintaining these infrastructures is seen as a critical issue, because the development of digital technologies has given data exchanges an important place in the formalisation of the global market, and transcontinental technical dependencies have intensified. So owning submarine cables or having specific skills in this area means having new powers and being able to exploit dependencies on these infrastructures. The owners of cables, and in particular the Big Tech companies that have invested massively in this field, have the capacity to influence not only access to the continent's resources, but also the technical, political and cultural aspects. To understand these new balances of power, this article first looks at the conditions of interdependence that give submarine cables their important place today. It then goes on to analyse the strategies of dependence and technological subjugation, using the example of Africa, which is now the expansion ground for the new cable owners.

**88   Satellite imagery and sovereignty: from the data to
its exploitation, towards a public-private continuum**
François BOURRIER-SOIFER

The notion of sovereignty has recently regained a central place in public debate, without however really renewing the dichotomy of State action between a patrimonial conception (dominium) and control (imperium). However, in the satellite imagery sector, given the rise of New Space, it seems that the optimum approach might be to favour a form of hybridisation between ownership and impact, from the data to its exploitation. To this end, the State should pursue the creation of an ecosystem based on a form of public-private continuum. This would maximise the desired end effect: power in action, dictated by the imperative of strategic autonomy.

COURSES OF ACTION AND LEVERS

94   Public procurement: an accelerator of digital sovereignty
Jean-Noël de GALZAIN & Alain GARNIER

Public procurement plays a crucial role in promoting digital sovereignty. The massive adoption of digital tools during the pandemic has made companies more dependent on large foreign platforms. To preserve our autonomy and our ability to excel in a world dominated by AI, it is essential to make greater use of French or European solutions in public procurement, particularly for strategic purchases and the protection of sensitive data.

By positioning itself today on sovereign digital solutions, France can regain control of its personal and industrial data, thereby guaranteeing its freedom, autonomy and capacity for innovation. The State can play a more directive and coercive role in encouraging the adoption of sovereign solutions in public administrations and companies.

The future will depend on decisions taken at European level, but France can set an example by moving forward on the road to digital sovereignty.

99 Global Internet governance: the levers
Lucien CASTEX

The digital transformation of society has turned the Internet into an everyday object, a combination of uses and technical artefacts. Its governance is characterised by an ad hoc model borrowing from multipartism, multilateralism and the uses of the network. Today, this governance is disputed, at the heart of a power struggle over the network of networks.

103 Changing cyber postures: how China, Russia, the USA and the EU see the world
Rayna STAMBOLIYSKA

Some technological advances are so significant that they fracture our understanding of the world. Experts and policy-makers are beginning to dissect, albeit sometimes timidly, the potential consequences of adding unfamiliar, advanced and potentially devastating new technologies to the toolbox of opposing powers. In this context, cybersecurity postures are particularly attractive. These postures provide a better understanding of the strategic changes underway among the main players on the geopolitical chessboard. We examine China, Russia, the United States and the EU through the prism of their cyber postures, which reflect the civilisational visions that determine the future actions of these players. These strategies reflect the long-term perspectives of these actors, offering insight into their motivations and possible blind spots that need to be taken into account.

108 Digital, an ambivalent power: what strategic autonomy for Europe?
Hugues de JOUVENEL & Jean-François SOUPIZET

The authors begin by pointing out how the rise of digital technology is a veritable revolution that is spreading to all areas and giving the Internet giants unprecedented power over governments and international institutions. They then show how these technologies bring opportunities but also risks that require constant vigilance, if not a capacity for anticipation, which is unevenly distributed. Finally, they highlight the limits of Europe's strategic independence and outline three hypotheses for the future of its "strategic autonomy".

113 Digital sovereignty without the State: is there individual sovereignty for "homo numericus"?
Pierre NORO

The concept of "digital sovereignty" usually refer to nation-states, their ability to provide for their digital needs, and occasionally to "Big Tech" companies they often depend on. However, considering the ideological roots of the Internet, the advocacy work of digital rights activists, and the practices of various communities revolving around FOSS, encryption or blockchain technologies, digital tools might primarily be technological foundations for users to claim a new form of sovereignty for themselves.

This article aims to outline this concept, probing its meaning and historical legitimacy. Beyond a limited initial definition of a de facto self-sovereignty, the

creation of tools to actualize universal values and freedoms gives substance to an "individual digital sovereignty" articulated around digital commons and deriving its legitimacy from their open governance. This emerging sovereignty locally competes or converge with the ones of nation-states and of platform companies.

122 The law to serve EU digital sovereignty
Brunessen BERTRAND

There is internal tension within the European Union over the idea of digital sovereignty, with some states more reluctant to commit to a real political vision implied in a digital sovereignty project. The ambivalence of European digital regulation illustrates the delicate balance between the political affirmation of the European Union through law, and the desire not to inhibit too much, through overly restrictive regulation, the technological innovations it needs in an international geopolitical context where it sometimes struggles to find its place and assume its singularity.

MISCELLANY

127 Cryptocurrencies and the passion for secrecy
François VALÉRIAN

Cryptocurrencies have developed over the past 15 years, benefiting from a passion for secrecy and a desire to abolish government control. This has created vast opportunities for the financial crimes that opacity allows, among which money laundering. More government is needed, more of a state whose financial regulation serves the needs of citizens, not the "less government" claimed by the first promoters of cryptocurrencies. More government, and more global regulation, since the financial world is global whereas the political world is fragmented.

Issue editor
Julien NOCETTI