STORMSHIELD

OPINION ARTICLE

CAN EUROPEAN DIGITAL SOVEREIGNTY REALLY EXIST?

Pierre-Yves Hentzen
Chief Executive Officer,
Stormshield

The term digital sovereignty is regularly heard in political discourse. However, in a globalisation context, where each nation is dependent to varying degrees on others, the challenges to achieving such sovereignty are immense. Thus, the cloud economy, cybersecurity and the control of essential digital infrastructures have become major stakes in a turbulent competition between nations wishing to secure their future. Can Europe emerge sovereign or is digital sovereignty simply a utopia?

In September 2021, during a press evening held on the fringes of the Assises de Monaco, a round table discussion raised this issue: "*The 2024 Olympic Games: how is the French team preparing for cybersecurity issues?*" This is a fundamental question, particularly since the announcements of the International Olympic Committee (IOC), which chose the cloud solutions of the Chinese giant Alibaba. This is a major inconsistency, so much so that the subject is considered "*very serious*" by **Bernard Le Gorgeu**, sector coordinator for major sports events within the French agency ANSSI. **Ziad Khoury**, national prefect coordinator for the security of the Olympic Games, recalled the commitment of the Ministry of the Interior "to promote French knowledge" and its attachment "*to the idea of digital sovereignty*"

LONG-DESIRED DIGITAL SOVEREIGNTY

The notion of digital sovereignty appeared in France in 2011, under the impetus of **Pierre Bellanger** who defined it in an opinion piece: "*Digital sovereignty is the mastery of our present situation and our destiny as manifested and directed by the use of computer technologies and networks*". Since then, the notion has flourished in all political programmes and has shaped the speeches of many ministers, secretaries of state in charge of digital issues, and even the President of the Republic.

This desire to defend the country's digital sovereignty can already be explained by the importance of the digital economy: in France for example, it represents more than 6% of the GDP (nearly 150 billion euros). On the other hand, the public's desire for independence is extremely strong: 87% of French people want to reduce France's economic dependence on foreign countries. But **should this reflection be carried out at the national or European level?** "*Even if this can be done at national level, this desire for digital sovereignty must be met by a common response at European level and by awareness when making investments or purchases,*" explains **Florian Bonnet**, Director of Product Management for Stormshield. *And to date, Europe's strategy is to reduce its members' dependence on non-European technology and capital, but is this enough?"* This view echoes some of the other positions taken by experts, pushing for the creation of European champions. On this basis, if European digital sovereignty is to be achieved one day, it should be through **the creation of these champions** on three major fronts: the cloud, cybersecurity and infrastructure.

CLOUD: EUROPE STRIKES BACK

Looking at the state of the cloud market, American dominance is clear. Currently, Amazon, Microsoft and Google jointly share 69% of the European cloud against less than 2% for the leading European players (of which OVH is the French champion). With a growth rate of 25% per year, this market is expected to be worth almost 500 billion euros by 2030... Beyond the ideal of sovereignty, there is also a colossal challenge of repatriating the creation of digital value in Europe.

But how do we move the lines? In an attempt to address this, the EU adopted the so-called General Data Protection Regulation (GDPR) in April 2016 (to be implemented in May 2018). The primary aim of the text is therefore to protect European citizens with regard to the processing of their personal data. But it also creates a regulatory environment in which European technological solutions can flourish more easily (as they are supposed to be the first to comply with the regulation). This regulatory approach is also reflected in the European NIS Directive. With it, cloud service providers must comply with an obligation of security and provide more guarantees on data control, reversibility, IT security and sovereignty. Opposing foreign champions through mere legal regulations? However, the idea is not unanimous in Europe, where many are alarmed at the EU's defensive response, when it should be going on the offensive. **Cyrille Dalmont**, associate researcher at the Thomas More Institute, does not hesitate to compare the GDPR to a "*Maginot Line*" of the digital world and to underline its complete ineffectiveness in "*building an improbable European sovereignty which it would guarantee*". The GDPR would thus further penalise European VSEs and SMEs by having "*virtually no impact on the global digital giants*". According to him, Europe has since been constantly compensating for the shortcomings of the GDPR by adding new regulations (including the Digital Services Act and the Data Governance Act). This "*normative inflation*" would lead to "*mortifying inertia*" when the EU should rather "*encourage the constitution of European digital champions*". And to protect them, like the US and the Alibaba Cloud investigation.

In parallel to the EU-wide regulatory measures, some governments (mainly in France and Germany) are adopting **more committed retaliatory measures**. Recently, the state of Schleswig-Holstein in Germany announced its intention to abandon the use of Microsoft's Windows operating system and all of its Office tools in favour of open source solutions on Linux and LibreOffice. The same is true of the French Interministerial Directorate for Digital Affairs (DiNum), which has sent a memo to all the general secretaries of ministries to remind them of the non-compliance of Office 365: "*The collaborative, office automation and messaging solutions offered to public officials are systems that handle sensitive data. Thus, the migration of these solutions to Microsoft's Office 365 offer is not in line with the Cloud at the Centre policy*". This "Cloud at the Centre" policy sets out the French government's roadmap for making the cloud "*the default hosting and production mode for the State's digital services*" and for public players, including major issues of sovereignty and security. It stipulates in black and white that "*the adoption of the cloud must not hinder the State's autonomy with respect to decision-making and action, nor its digital security and the resilience of its infrastructures, the State's control of the data and processing entrusted to it, or its compliance with European rules on the protection of personal data, and this at a time when the footprint of non-European players in the field of the cloud is predominant*".

> *"Are American interest representatives best placed to develop and present what European sovereignty should be?"*
>
> **Léonidas Kalogeropoulos**, General Delegate of the Open Internet Project

But while some in Europe are trying to adopt this approach, this is often met with **aggressive lobbying by foreign players**. **Yann Lechelle**, general manager of Scaleway, will certainly not contradict him. The company is one of the 22 founders of the Gaia-X project, which aims to build a European sovereign cloud. The company director has however made it official that his company is withdrawing from the project, denouncing it as a sham under American and Chinese influence. Indeed, companies such as Amazon, Google, Alibaba or Palantir were asked to be sponsors. "*Would it be conceivable for an Alcoholics Anonymous association to be sponsored by a spirits group?*" asks Yann Lechelle.

Europe is making a fool of itself. “*Can Europe really claim to ensure its sovereignty by creating a digital NATO by 2030?*” asks Florian Bonnet. **Jean Noël de Galzain**, President of Hexatrust and Wallix Group, also testifies to the power of influence that GAFAM and BATX have. In an article, he denounces the Thales-Google Cloud agreements “*for the creation of a joint venture to provide an offer that meets the criteria of the “trusted cloud” label, in accordance with the French national strategy*”. This battle for influence is even deeply rooted in the debates around the very definition of digital sovereignty, for which some advocate for an approach open to foreign players. In a press release issued in early February 2022, **Leonidas Kalogeropoulos**, General Delegate of the Open Internet Project, asks: “*Are American interest representatives best placed to develop and present what European sovereignty should be?*”

CYBERDEFENSE: FRANCE INTENDS TO GET EUROPE UP AND RUNNING

This “Cloud at the Centre” policy is also a symbol of the **convergence of cybersecurity and cloud issues**, since it makes it imperative to host digital products handling sensitive data “*on the State’s internal cloud or on a commercial cloud policy as SecNumCloud by the ANSSI*”.

This convergence is not insignificant. Indeed, if Europe is to achieve the digital sovereignty to which it aspires, it will certainly need to be able to protect it. However, at the International Cybersecurity Forum held in Lille last September, **Margarítis Schinás** widely communicated the fears of the highest European authorities in the field of cyberdefense. The Vice-President of the European Commission described “*a critical situation*” and the “*recent increase in cyberattacks by international players*”, which would have **dramatic consequences for public services and therefore for the stability of Europe**. France, which has taken over the leadership of the Council of the European Union, has already expressed several times its intention to restructure the EU to provide it with adequate cyberdefense capabilities. At the European level, France no longer wishes to talk about cybersecurity, but rather about cyberdefense. The stakes are becoming military, as shown by the intervention of **Florence Parly**, the French Minister of Defence, who questioned the resurgence “*of a cold war in cyberspace*”. France has announced the reinforcement of its digital warfare contingent and thus wishes to become “***a European cybersecurity champion***”. With the ambition of persuading the entire European Union to structure its defence capabilities in the same way.

While such speeches underline the extent to which cybersecurity is taken seriously in the defence of European sovereignty, Europe is currently structuring itself with new legislation... The European Parliament and Council are currently examining the revision of the NIS 2 Directive (related to the security of networks and information systems), which should considerably extend the list of sensitive sectors. While the list of Essential Service Operators (ESOs) has so far been left to the discretion of the Member States, the NIS 2 Directive will impose the criteria by adding new sectors (postal services, waste management, large-scale food distribution, etc.) to the areas already included (such as banking, energy, health, etc.). Another important development is that central and state administrations are officially included in the scope of the directive and become Essential Service Operators, while the addition of regional and local administrations is still left to the Member States.

INFRASTRUCTURE: A SILENT CYBERWAR

If the cloud and cybersecurity are the visible pillars of digital sovereignty, there is a third one, which is less attractive to the general public, even though it is the scene of a real hegemonic war, namely infrastructures.

In June 2019, at a hearing before the French Senate, the Interministerial Directorate of Digital Affairs (Dinum) warned: "*If we do not have players capable of producing the infrastructures, building the services, managing the first-level relationship with users and mastering the interfaces, we will probably be relegated to the second division in terms of sovereignty.*" The same year, in August, French Parliament passed a law often referred to as "Anti-Huawei" that severely restricted the authorisation of foreign economic players to support and operate mobile network bands. Although the aim was not immediately clear, the purpose of this law was to exclude Huawei and any other Chinese players from the race to install the network infrastructure that will serve as the basis for the future French 5G. France thus followed in the footsteps of Great Britain and Sweden (not to mention the United States under the Trump administration), which had all proceeded in a similar manner. This position is in line with that of the EU and its members' defensive policy regarding sovereignty.

But this infrastructure battle is not only fought over the airwaves; it is also fought in the sea. Today, 99% of intercontinental electronic communications transit via submarine cables. In a rationale of sovereignty, the European Union must ensure that these infrastructures do not fall under the control of foreign entities. However, since this sector is poorly regulated (precisely in a rationale of state neutrality), private players from all over the world are rushing to take control of it. Traditionally owned by consortia of telecoms operators (many of them European), the American GAFAMs have entered the race with unprecedented strength in the last decade. **Jean-Luc Vuillemin**, director of international networks at Orange, notes the alarming evolution in an interview: "*Ten years ago, 5% of submarine cables were controlled by GAFAMs. Today, the figure is 50% and it will be 95% within three years*." This entryism of the major American digital platforms, which are being followed by the Chinese BATXs, has transformed the sector into a "*real Wild West*", where the law of the strongest prevails over common interest.

The evidence is clear: from its infrastructural base to its value creation, **the European digital field is far from being sovereign and is increasingly subject to foreign pressure**. While the notion of digital sovereignty is an understandable ideal from both an economic and geopolitical point of view, the European Union currently seems to be choosing the path of over-regulation. Before moving up a gear? This is at least the signal sent by the European Commission, which just launched a call for projects worth 80 million euros at the beginning of 2022 for the creation of a European DNS resolution service.