**CAUGHT IN THE WEB: THE DIGITAL SOVEREIGNTY**

In the current scenario, where the Internet is increasingly present in everyday life, complex and contentious discussions surrounding the concept of digital sovereignty are becoming more prominent. This multifaceted and controversial topic involves the capacity and right of entities, be they nation-states, organizations, or groups of individuals, to exert control and authority over their digital environment independently and autonomously from other sovereign entities.

This article is a condensed version of the project I presented at ICANN 78 as a [NextGen participant](https://icann78.sched.com/event/1T4O9/nextgen-presentations-2-of-2). It represents the first step towards a more in-depth analysis of this concept to explore its implications on society, particularly on the critical properties of the Internet.

First and foremost, it's essential to recognize that the debate on digital sovereignty is evolving, and this article seeks to shed light on the dimensions and inherent challenges of the topic.

One of the most pressing challenges related to digital sovereignty is finding ways to apply it while simultaneously safeguarding the open, global, and accessible nature of the Internet. This duality between digital sovereignty and preserving the Internet as we know it is essential to ensure that it continues to be a valuable resource for humanity.

Hence, the challenge lies in finding a means to ensure that states and other entities can responsibly and effectively control their digital environment. Therefore, it is imperative to find ways to balance digital sovereignty with the preservation of the critical properties of the Internet.

But what are the critical properties of the Internet?

The Internet is a global interconnected network of computers built upon a set of critical properties fundamental for its efficient operation and for preserving its global and open nature. Following [the proposal](https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf" \t "_blank) of the Internet Society (ISOC), these critical properties can be divided into five main categories: (i) Accessible Infrastructure with a Common Protocol; (ii) Open Architecture of Interoperable and Reusable Structural Blocks; (iii) Decentralized Management and a Common Distributed Routing System; (iv) Common Global Identifiers; (v) a General-Purpose Network.

These critical properties underpin the global and open nature of the network, allowing for its continuous expansion, adaptation, and innovation. Accessible infrastructure with a common protocol ensures global connectivity and encourages the growth of the Internet, making it accessible to all. Open architecture promotes interoperability and innovation, while decentralized management and a distributed routing system ensure a resilient and adaptable network. Common global identifiers provide consistency and cohesion, preventing network fragmentation. Lastly, a general-purpose network enables the Internet to serve a diverse community of users and applications while remaining flexible in the face of change.

But how can applying different notions of digital sovereignty impact these critical properties?

First, it is necessary to understand the different concepts and notions of digital sovereignty. Among the various concepts of digital sovereignty, here we will address three of them: (i) as state power, (ii) as developmentalism, (iii) as autonomy and self-determination of groups and individuals.

Digital sovereignty as state power can be understood as an element of the [power of a nation-state](https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf" \t "_blank). It pertains to the control of digital infrastructure, such as telecommunications networks and servers, and the ability to establish norms and regulations for the Internet within the country. This approach often focuses on national security and controlling the flow of information, which can lead to measures such as censorship, surveillance, and even the complete or partial shutdown of the Internet in times of crisis. It is a concept that places the State at the centre and is generally thought of as hierarchical or "top-down".

Another concept of digital sovereignty, known as developmentalism, is understood through an economic lens. This perspective of digital sovereignty is more oriented toward a [country's economic development](https://d-nb.info/1270381776/34" \t "_blank). Here, the emphasis is on reducing dependence on foreign companies, especially tech giants, and promoting local technology and services, either through government initiatives or by national industries/companies. A clear example is when there is an incentive to use domestic technologies and establish national digital infrastructure. This aims to achieve greater economic autonomy and competitiveness in the global market.

A third concept of digital sovereignty relates to the [ability of individuals and groups to exercise control](https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf" \t "_blank) over their data and decisions in the digital environment. This involves using open-source technologies and services and respecting cultural preferences and individual values when dealing with personal data and information. This approach values autonomy and the capacity of people to decide how their data is collected, used, and shared. This concept has a strong "bottom-up" connotation, especially with the idea of empowering and building infrastructure from the community.

The choice between these approaches has significant implications for Internet Governance, the protection of individual rights, and the dynamics of international relations in the digital world.

 In the case of digital sovereignty as State Power, the emphasis is on the control and authority of the State over various layers of the digital environment, including physical infrastructure, code, software, and operational protocols. These policies are often used to justify state sovereignty and the defence of national security. However, [their effects](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993485" \t "_blank) often lead to censorship, surveillance, human rights violations, and the risk of Internet fragmentation when these actions impact critical structures of the Internet.

On the other hand, the developmentalist approach also presents risks when seeking to create greater economic autonomy and competitiveness, as it can lead to technological isolation, lack of universal standards, risks of censorship, and Internet fragmentation.

The approach of autonomy and self-determination of groups and individuals also has a high potential for complexity if not supported by open-source technology and code development, potentially resulting in a lack of universal standards, economic implications, and cybersecurity risks.

In all of these approaches, there are potential risks to the critical properties of the Internet, such as accessibility, interoperability, decentralization, common global identifiers, and a general-purpose network.

Therefore, the choice of a digital sovereignty concept must be carefully evaluated in light of these risks to ensure that the Internet remains global, open, and accessible to all.

To do so, the first step is to conduct a detailed analysis of the impacts and risks that digital sovereignty policies may have on the critical properties of the Internet. This includes identifying threats such as censorship, surveillance, network fragmentation, and the lack of universal standards. It is important to understand how each digital sovereignty approach affects accessibility, interoperability, decentralization, common global identifiers, and the overall nature of the network.

After the initial analysis, engaging the global community in open and transparent debates is crucial. These discussions should take into account the results of the impact and risk analysis. Beyond local and regional Governance Forums, this discussion should also take place in spaces for the development and formulation of public policies, not limited to the participation of experts or the government but involving multiple stakeholders that make the multistakeholder model effective.

Civil society organizations play a crucial role in advocating for the rights of citizens regarding the Internet. Creating an enabling environment for civil society participation is essential, ensuring that their voices are heard at the local and regional levels. Additionally, educating local communities about digital sovereignty issues is fundamental. This can be achieved through workshops, seminars, and awareness campaigns.

Transparency is essential throughout the process. Policies and decisions related to digital sovereignty must be transparent, allowing the global community to understand how they are being formulated and implemented. Furthermore, accountability mechanisms must be established to ensure policies are implemented fairly and equitably.

The need to adopt common approaches to common problems at the local, regional, and global levels is fundamental to address the challenges of digital sovereignty effectively. By adopting common approaches, such as the use of widely accepted technical standards, it is possible to promote global connectivity and accessibility. Cybersecurity challenges are common to all countries and regions. A common approach involves global collaboration in identifying threats and adopting best practices to protect critical infrastructures.

However, it is equally important to recognize and balance local and regional contexts in developing these public policies. Digital sovereignty policies must take into account cultural diversity and local values. What may be acceptable in one cultural context may not be in another. Therefore, it is important to allow policy flexibility to accommodate these differences.

Successful local practices and best practices can be shared globally. What works well in one country or region can serve as a model for others, promoting innovation and policy effectiveness. Therefore, when developing common approaches to common problems, it is important to balance global collaboration and respect for local and regional contexts. This will ensure that digital sovereignty policies are effective and sensitive to the needs of communities worldwide while effectively protecting the critical properties of the Internet.

The creation of laws and regulations should be seen as a last resort, to be applied only when other approaches fail to protect the critical properties of the Internet. It is essential to ensure that any regulation is carefully crafted and considers all stakeholders' interests. Coercive regulation should be avoided whenever possible to preserve the open nature of the Internet.

Ultimately, digital sovereignty is a challenge that must be overcome through collaboration and balance among the needs, duties, and rights of all stakeholders involved and the preservation of the essential characteristics of the Internet. By adopting a responsible and collaborative approach, we can ensure that the Internet remains a valuable resource for humanity.