

Beyond Sovereignty:
Strategies for Digital Autonomy in the Southern Cone

Lucía Bosoer

Thesis submitted for assessment with a view to obtaining the degree
of Master of Arts in Transnational Governance of the European
University Institute

Florence, 15 May 2022

European University Institute
School of Transnational Governance

**Beyond Sovereignty:
Strategies for Digital Autonomy in the Southern Cone**

Lucía Bosoer

Thesis submitted for assessment with a view to obtaining
the degree of Master of Arts in Transnational Governance
of the European University Institute

Supervisor

Daniel Innerarity

Chair AI&DEM STG European University Institute Florence
Ikerbasque Foundation for Science, UPV/EHU, Globernance

© Author, [2022] . This work is licensed under a [Creative Commons Attribution 4.0 \(CC-BY 4.0\) International license](https://creativecommons.org/licenses/by/4.0/)

If cited or quoted, reference should be made to the full name of the author, the title, the series, the year, and the publisher.

**Student declaration to accompany the submission of written work
School of Transnational Governance**

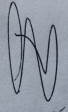
I <Lucía Bosoer> certify that I am the author of the work <Beyond Sovereignty: Strategies for Digital Autonomy in the Southern Cone> I have presented for examination for the Master of Arts in Transnational Governance. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297)).

The copyright of this work rests with its author. Quotation from this thesis is permitted, provided that full acknowledgement is made. This work may not be reproduced without my prior written consent. This authorisation does not, to the best of my knowledge, infringe the rights of any third party.

I declare that this work consists of <10437> words.



LUCÍA BOSOER
FLORENCE, 15 MAY 2022

ABSTRACT

Faced with the multiple challenges posed by the digital transition, different regions, countries, and communities around the world have conceived strategies to uphold their “digital sovereignty”. Yet, the meanings and implications of such digital sovereignty are unclear, and concepts that may be appropriate in one context may be misleading or obfuscate a needed public debate in another. This research aims to explore the specific challenges of the advance of digital technologies in the Southern Cone through an alternative conceptual approach: the Latin American School of Autonomy. It will attempt to outline the main barriers facing the region in this area and elucidate possible ways forward in the path towards digital autonomy. In a context of international fragmentation around the governance of digital technologies and rising US-China technological competition, the strategy that emerges as the most appropriate for Southern Cone countries in the coming years is that of limited containment.

Keywords: digital sovereignty, school of autonomy, Southern Cone, limited containment

TABLE OF CONTENTS

1. Introduction	3
2. Digital sovereignty: An overview of a contested concept	6
2.1. <i>How did digital sovereignty become trending topic?</i>	6
2.2. <i>Digging into the content</i>	8
3. From Sovereignty to Autonomy in South America	14
3.1. <i>The School of Autonomy</i>	15
3.2. <i>Relational autonomy</i>	16
4. Methodological approach	20
5. Findings and discussion	22
5.1. <i>Positions regarding digital sovereignty</i>	22
5.2. <i>Main identified barriers</i>	25
5.3. <i>Variances within the region</i>	27
5.4. <i>Strategies towards digital autonomy</i>	28
6. Looking forward	35
References	37

1. Introduction

In February 2014, during a European Union (EU)-Brazil summit held in Brussels, the then President of Brazil Dilma Rousseff announced the laying of an undersea cable linking its country and Europe. The initiative came on the heels of Edward Snowden's 2013 disclosures, which showed that the United States (US) National Security Agency (NSA) had carried out a global surveillance program under which, among many other things, it had accessed emails, text messages and phone conversations of President Rousseff, her aides, and other important Brazilian figures. Given that the NSA had accessed much of the information through the tapping of fiber optic cables (Khazan, 2013), Rousseff's announcement came as a surprise to no one. "We have to respect privacy, human rights and the sovereignty of nations," she stated on that occasion, showing that technological projects are rarely detached from political and strategic considerations. The cable, named EllaLink, became operational in 2021. It is the first to directly connect South America with Europe; previously, most fibre-optic cable connections between the two regions passed through the US (EllaLink, 2021).

The advance of digitalisation and emerging technologies presents unparalleled opportunities for humanity, but also great challenges that require a comprehensive and interdisciplinary approach. The patterns that have shaped the digital transformation of the past two decades have led several scholars to note the emergence of a new global socio-economic model based on the extraction of raw materials, labor, and human data (Kwet, 2019; Zuboff, 2019; Crawford, 2021). Under this new model, the entire human experience is being datified, to be processed and converted into revenue streams¹. The increasing extraction, appropriation, processing, and manipulation of human data has allowed a few technology companies, most of them from the US, to accumulate

¹ The obscure and complex processes through which this occurs are beyond the scope of this paper, but they are no less important. Indeed, they represent a fundamental aspect of how human life and societies are organized today (Lyon, 2015; Zuboff, 2019; Crawford, 2021).

a concentration of power without precedents in modern history². According to Couldry and Mejías (2019), what the world is facing is not the advent of a new system, but rather the extension of colonialist and capitalist practices over new areas enabled by technological advances. The logic of data extractivism cuts across and complicates the traditional dividing line between North and South, but affects developing and least developed countries, the so-called Global South, on a much greater scale.

From a geopolitical perspective, digital technologies have become a core aspect of great power competition, and a growing number of studies consider the governance of digital technologies in terms of divergent models (Coyer & Higgott, 2020; Hobbs & Torreblanca, 2020; Ziebert, 2021). On the one side, there would be the US model led by the private sector and market principles; on the other, the Chinese path of tight state control of technological developments and censorship within its borders. In between both, the European model is presented as a “third way”, based on a regulated digital ecosystem and the protection of people’s fundamental rights (Colomina, 2021; Burrows et al., 2022). Faced with the increasing pervasiveness of digital technologies in all aspects of human life, the unbridled power of a few unregulated corporate players, and rising US-China competition, the EU has sought to develop a series of legal frameworks that allow it to preserve its “digital sovereignty” (Floridi, 2019; Pohle, 2020; Innerarity, 2021). Yet, the precise meanings and implications of such digital sovereignty are far from clear and the value of the concept has been called into question (Mueller, 2019). While for some it is a core element for nations’ self-determination in the current era, others see it as an excuse for authoritarian governments to control citizens.

In this complex scenario, the rest of the world, once again, seems to be relegated to the role of spectator or passive consumer of one of the above models.

² Currently, the GAFAM oligopoly - Google (Alphabet); Apple; Facebook (Meta); Amazon; and Microsoft - has a combined total market capitalization valuation larger than the combined Gross Domestic Product (GDP) of some of the world’s richest countries. In 2020, its valuation was more than twice the combined GDP of Africa (Mirrlees, 2020).

Still, while the nature and dynamics of digital transformation transcend borders and extend across the entire globe, the precise ways in which they interact and affect each region, country, or community may vary. The same holds true for how different people may perceive, experience, and respond to the opportunities and challenges posed by digital technologies (Milan & Treré, 2019).

Driven by this concern, this research aims to explore, from an international relations perspective, the specific challenges of the advance of digital technologies for a particular region of the world: the Southern Cone of the American continent. As the example of the EllaLink cable shows, the Southern Cone countries, namely Argentina, Brazil, Chile, and Uruguay³, have had a voice of their own in the “geopolitics of digital governance” (O’hara & Wall, 2018), and have developed specific policies that have remained under the radar of many studies. What has been the impact of these policies? What is the current state of governance of digital technologies in these countries? Is it even a relevant concern within their public agenda?

Through the gaze and voice of local actors involved with the impact of digital transformation in the Southern Cone, this thesis seeks to shed light on this region’s main challenges in developing an autonomous governance of digital technologies. It is structured as follows. Firstly, it provides a critical review of the concept of digital sovereignty, exploring its origins, the different geographies, and practices with which it is often associated, as well as the criticisms it has received. Secondly, it proposes to approach the question of digital policies in the region through the lens of the Latin American School of Autonomy, and in particular, relational autonomy (Russell & Tokatlian, 2003). Finally, it identifies the main challenges facing the region in this area today and outlines possible strategies to move towards digital autonomy.

³ The choice of the case studies is due to these four countries’ specific practices and policies in the field of digital technologies. Paraguay, generally considered part of the Southern Cone, was not included in the research, but it is assumed that the results found for these countries are also applicable to the Paraguayan context.

2. Digital sovereignty: An overview of a contested concept

2.1. *How did digital sovereignty become trending topic?*

During the 1990s and the first decade of the 21st century, with the collapse of the Soviet bloc, the growing power of non-state actors, and the advancement of globalization in all areas, the prevailing idea at both the political and academic levels was that the state, as the most important unit of the international order, was losing relevance. The explosion of the Internet and the growth of transnational data flows fed the interpretation of national borders as an outdated construct in the current globalized world. European policy circles spoke of a “global information society” (Glasze & Dammann, 2021, as cited in Glasze et al., 2022), and social media platforms were primarily seen as a democratizing force that gave voice to oppressed peoples around the world. Westphalian sovereignty seemed to be losing steam, and national borders appeared to be meaningless in a world of deep interconnections and transnational flows (Linklater, 1998; Ohmae, 1999; Habermas, 2001). In recent years, however, sovereignty has returned to the forefront of global discussions (Krastev, 2021). The world of digital technologies, convulsed by the 2007 cyber-attack on Estonia, the Snowden revelations, and the Cambridge Analytica scandal, between other major developments, did not remain on the sidelines of this debate. Since the early 2010s, the idea of “digital” or “technological” sovereignty began to take shape in political debates around the world.

In France, the concept of digital sovereignty started to gain prominence in the public debate in 2011, when the CEO of the French radio station Skyrock, Pierre Bellanger, called for making digital sovereignty (*souveraineté numérique*) a new expression of French and European freedom. In 2020, French President Emmanuel Macron claimed that Europe’s freedom of action depended on its economic and digital sovereignty, and called for strengthening European control of its critical infrastructure (Macron, 2020). In Germany, digital sovereignty started to be discussed at the highest political levels since the NSA surveillance

revelations (Glasze et al., 2022). In its program for the German EU Council presidency in 2020, the German government declared its purpose of establishing “digital sovereignty as a leitmotiv of European digital policy” (Bundesregierung, 2020, 8). Since then, digital or technological sovereignty has become a ubiquitous element in European strategic documents, plans and conferences addressing the future of the Union⁴.

Outside the so-called Western world, digital sovereignty has been one of the strategic priorities of the last ten years in both Russia and China, although in these two cases the concept that is most often used is that of cyber sovereignty. Sovereignty over digital infrastructure as an important element of the Russian public debate began to emerge in the early 2010s (Glasze et al., 2022). With the beginning of Putin’s third term, the Internet began to be seen as a sphere dominated by the US and allied countries, and thus as a threat to the interests of the Russian people. In the last ten years, a series of laws were passed that gave the state more power to centralize control over the internet infrastructure, block content deemed undesirable or dangerous, and isolate its cyberspace from the rest of the world (Sahuquillo, 2019). In the same vein, cyber sovereignty has been a pillar of the Chinese government’s strategic policy documents and international statements since the 2010 White Paper outlining China’s position on the Internet⁵ (Creemers, 2020). The Chinese government’s interest goes far beyond the control of content circulating in cyberspace, something it has already largely achieved. Its broader ambition is to challenge US primacy in the field of digital technologies at a global level, which has led observers to speak about a “tech cold war” between Washington and Beijing (Segal, 2020).

⁴Commission President Ursula von der Leyen defined technological sovereignty as “the capability that Europe must have to make its own choices, based on its own values, respecting its own rules” (Von der Leyen, 2020). Meanwhile, in March 2021, German Chancellor Angela Merkel, Danish Prime Minister (PM) Mette Frederiksen, Estonian PM Kaja Kallas and Finnish PM Sanna Marin, wrote in a letter to von der Leyen that the time had come for Europe to become digitally sovereign (ERR, 2021).

⁵According to the Wuzhen Declaration, distributed during the first World Internet Conference in 2014, countries should respect each other’s rights “to the development, use and governance of the Internet, [and] refrain from abusing resources and technological strengths to violate other countries’ Internet sovereignty” (WIC, 2014, as cited in Creemers, 2020).

While the quest for cyber sovereignty by authoritarian governments has been interpreted by the Western world as an excuse to exert greater control over their populations, the truth is that some of the discourses and practices of digital sovereignty in Europe, particularly those regarding data localization, share certain common features with the initiatives of these countries (Glaszle et al., 2022). Whether within liberal democracies or in non-democratic countries, the concept of digital sovereignty is becoming increasingly present in public debate. Yet, there is much confusion over its meaning and practical implications. For instance, digital sovereignty, cyber sovereignty, and data sovereignty are often used interchangeably, although they do not necessarily imply the same policies. Mueller (2019) argues that those who want to apply the notion of sovereignty to cyberspace are seeking to replicate traditional institutions in a whole new sociotechnical system. This is not only technically inadequate, as it ignores the complexity of cyberspace, but also dangerous, since such claims could ultimately lead to a fundamental reordering of cyberspace. He points out that many analysts confuse cyberspace with Internet or information technologies, and as each of these things “consist of complex combinations of private and shared physical facilities, commercial and noncommercial services, and multiple layers of open and proprietary standards and software” (Mueller, 2019, 23), the discussion around these issues is often obscured. Nor can cyberspace be equated with the “digital”, and thus cyber sovereignty cannot and should not mean the same as digital sovereignty.

2.2. *Digging into the content*

In its various definitions, the idea of digital sovereignty seems to involve some kind of control over digital content and digital infrastructure (Couture & Toupin, 2017), but this is as far as the consensus goes. The question of what it means to have digital sovereignty in a world in which states continue to have the last word in defining their internal and external policies, but which has

undoubtedly been radically altered by data flows and the global nature of the Internet, seems to open up a wide range of definitions and rationales. As Glasze et al. (2022) argue, while seeking a single meaning for digital sovereignty is unlikely to be a simple or even useful task, “an examination of the genealogies of the concept can help us better understand the paradoxes and challenges of the contemporary ‘digital sovereignty’ debates” (p. 4).

The traditional notion of sovereignty was born in the 16th century with the political philosopher Jean Bodin, who thought about sovereignty as the supreme power of the ruler over the citizens, without constraints. Two centuries later, Jean-Jacques Rousseau updated the concept; the sovereign subject shifted from the ruler to the people, who were the ultimate power holders and who entrusted it to the ruler or the government. Today’s prevailing understanding of sovereignty tends to be linked to the Peace of Westphalia, although the modern international order based on sovereign states came much later (Krasner, 2001). In international law, external sovereignty refers to the independence of states from each other, while internal sovereignty means states’ right to self-determination (Pohle, 2020). Beyond the debate as to whether sovereignty is a standing international principle, or a myth created to be respected only when it is convenient to do so (Krasner, 1999), the problem that concerns this paper is that of applying a concept that is usually associated with a specific geographic space to the digital world. The key question is whether the logics of the analogue world also govern those of the digital world, and whether sovereignty in the former implies the same as in the latter.

In their attempt to bring some clarity to the debate, Pohle and Tiehl (2020) proposed one of the first systematizations of digital sovereignty claims. Focusing on the sovereign subject, they identified three distinct categories; those that refer to the digital self-determination of states, that of national companies, and that of individuals. Depending on the sovereign agent, the tools for achieving sovereignty may differ. The first category is the one that is the most present in political debates. It refers to the capacity of a state or region to preserve its

autonomy with respect to technological developments and digital infrastructure. One of the most relevant policies from this perspective has to do with control over data flows. The various data localization initiatives that have emerged in the last few years “seek to restrict the storage, movement and/or processing of data to specific areas and jurisdictions and are typically justified by the need to limit the access that foreign intelligence and commercial agencies may have to specific types of data” (Pohle & Tiehl, 2020, 9). The Court of Justice of the European Union (CJEU) judgment in the Schrems II case could be framed within this logic. In July 2020, the CJEU invalidated the EU-US Privacy Shield, the legal framework for regulating transatlantic exchanges of personal data for commercial purposes, after considering that it did not provide sufficient protection (Court of Justice, 2020). Beyond the legal and commercial implications of the ruling, the Schrems II case is a prime example of how transatlantic data transfers have become an area of strategic value for the EU.

A second but closely interrelated category of digital sovereignty claims focuses on the autonomy of national economies in regard to foreign companies and technology service providers. The policies adopted under this category are usually part of a much broader national strategy aimed at the digital transformation of the economic, commercial, and industrial sectors. It is mainly about capitalizing on the benefits offered by the digital economy by promoting the local business environment. According to the authors, a project that seeks to strengthen digital sovereignty from this economic perspective is the Gaia-X initiative for the development of a European cloud service⁶.

The third and last layer of digital sovereignty claims departs from a state-centered understanding of the concept of sovereignty, and instead emphasizes the importance of individual, citizen, and user self-determination. This category,

⁶Gaia-X would offer European citizens and companies an alternative to the world’s most powerful cloud service providers which are mostly US-based. However, the initiative also aims to keep a larger amount of European data within EU borders, and in this sense, it is also driven by security concerns. As such, it could be argued that Gaia-X is a good case in point of how security and economic considerations are intertwined when defending European digital sovereignty.

prevailing among activists and civil society organizations, views sovereignty as “the ability of individuals to take actions and decisions in a conscious, deliberate and independent manner” (Pohle and Tiehl, 2020, 11). It is about “technologies developed from and for civil society” (Haché, 2014, 11). The aim here is not to strengthen the autonomy of a state or region by promoting its local economy or regulating the information accessed by foreign actors, but to empower citizens by making them active agents in the design, implementation, and oversight of emerging technologies. The “tools” can be very varied and range from the development and implementation of free software and hardware to the promotion of digital literacy programs on a large scale. Unlike the first two categories of digital sovereignty claims, which assume a top-down conception of sovereignty, this third category assumes a bottom-up conception and tends to be based on a mistrust on the part of the user towards any kind of power and authorities, be they foreign companies or specific governments. Thus, Pohle and Tiehl (2020) identify three types of subjects who, according to the different calls for digital sovereignty, should maintain or regain a certain power in the face of the material – servers, undersea cables, hardware – and immaterial – code, data profiling practices, deep fakes – dynamics that the digital transformation entails.

Another approach to this same debate looks at the growing power of large tech companies, which threatens the traditional notion of state sovereignty, both internally and externally. Bremmer (2021) argues that the international order that has prevailed for the past 400 years is beginning to change, giving rise to a new world in which large technology companies take on the roles and responsibilities that were previously held by states. In this new order, the biggest US and Chinese tech companies “exercise a form of sovereignty over a rapidly expanding realm that extends beyond the reach of regulators: digital space” (Bremmer, 2021). At best, states have now become dependent on big tech companies to provide a range of public services, and at worst, these companies are directly providing and operating the services. Furthermore, in some cases these companies are

attempting to mirror state structures within themselves⁷. In contrast, Walt (2021) challenges this diagnosis. Without neglecting the increasing influence of big tech companies, he argues that states remain the dominant political unit of the international order. Tech giants may have an increasing power over digital space, but the latter, unlike physical space, is not essential to the future of human life. States remain the bedrock on which social life is structured in the physical world. Even in the digital space, companies are still subject to laws and regulations imposed by states. “When emergencies arise—9/11, the 2008 financial crisis, a catastrophic weather event—people don’t call Tim Cook or Sergey Brin to fix the problem; they turn to the government” (Walt, 2021).

The concept of digital sovereignty raises more questions than answers. Not only is there no consensus on the sovereign subject, or on whether it makes any sense to use notions created for the analogue world to explain the logics of the digital universe, but it is also unclear what the latter implies. As emerging technologies advance, the “digital” becomes increasingly complex and difficult to grasp. Attempting to apply universal notions to radically different contexts, in turn, makes the debate even more difficult. Just as digital or cyber sovereignty is interpreted one way in authoritarian countries and in a completely different way in democratic countries, the idea of greater control over data flows by the state may raise concerns in developing countries where there tends to be less trust in public institutions. Concepts that may be appropriate in one context may be misleading or obfuscate a needed public debate in another. According to Becerra and Waisbord (2021), digital sovereignty has not been a concern of Latin American countries in recent times. This could be explained, among other reasons, by the fact that “cybernationalism and sovereignty are tied to the geopolitics of world superpowers” (Becerra & Waisbord, 2021, 75). The production of knowledge is far from being neutral, and has always been traversed by relations of power, domination, and subjugation. As Couture and Toupin (2017) argue, whenever the idea of sovereignty related to the digital is

⁷Facebook (now Meta) Oversight Board, for example, is a body to which users can appeal to object to Meta’s content moderation practices on Facebook or Instagram. Simply put, it is a Court of Justice within Facebook.

included in a discourse or article, it is worth asking: “Who defines technological sovereignty and for which purpose it is pertinent?” (Couture & Toupin, 2017, 4). Surely the answer will be different in each case.

3. From Sovereignty to Autonomy in South America

Digital sovereignty has become a clear case of what Giovanni Sartori called “concept stretching”: its meaning has been so expanded that it is no longer clear what digital sovereignty really means (Mair, 2008). In the following sections, I will approach the problem of digital sovereignty in the Southern Cone from a perspective of international relations that emerged in the second half of the twentieth century in Latin America; the School of Autonomy⁸. The traditional relations of economic and political dependence of Latin American countries *vis-à-vis* the US involved not only the transfer of policies (Porto de Oliveira et al., 2019), but also the adoption of foreign conceptual frameworks to analyze the problems facing the region. This has never implied an absence of theoretical development at the local level, only that it has not always been given the relevance it deserves. At the same time, most critical analyses of the patterns that have underpinned the technological transformation of the last two decades tend to take liberal democracies as their frame of reference, “with their sociocultural substrate and long tradition of representative institutions, rule of law, and citizen involvement in public affairs” (Milan & Treré, 2019, 2). This has often translated into a disregard for the specificities and idiosyncrasies of other regions, localities, and communities around the world, and how these affect and are affected by digital technologies. Adopting the framework of the school of autonomy to discuss the digital transformation in the Southern Cone from an international relations perspective constitutes an attempt not only to overcome the limitations of the concept of sovereignty when applied to the digital world, but also, and even more importantly, to analyze the topic through a model that is more in line with the realities of the region, and its position and goals in the international scenario.

⁸ While this paper focuses on the Latin American School of Autonomy, it is worth pointing out that the pursuit of autonomy has been a central foreign policy objective of states for centuries. In recent years, the concept of strategic autonomy has also gained prominence in European policy debates (Tocci, 2021), and many of the points raised in those contexts relate to ideas developed within the Latin American School of Autonomy.

3.1. *The School of Autonomy*

The question of autonomy occupied a central place in theoretical and political debates in Latin America between the 1960s and the 1980s. The two main schools that reflected on the topic came to be known as “peripheral autonomy” and “peripheral realism”. Taking elements from the dependency theory developed out of the UN Economic Commission for Latin America and the Caribbean (ECLAC) a decade earlier, the school of peripheral autonomy was premised on the assumption that the international order had predominantly negative effects on the region, but that its countries had certain margins for action that could be capitalized upon (Russell & Tokatlian, 2010). Essentially, the idea of autonomy referred to broadening the margins of one’s own decisions and actions in the international arena. Internally, autonomy was seen as a way of protecting against the most negative effects of dependence, particularly in the economic realm. Externally, it was a tool for promoting one’s own interests in the international system (Tickner, 2014).

According to Jaguaribe (1979), the autonomy of the countries of the region depended on two main variables: national viability and international permissibility. National viability referred to a country’s possession of human, material, and strategic resources. International permissibility alluded to the character of the international system at a given moment and the capacity of a country to neutralize external threats (Tickner, 2014). The need for a certain degree of political and economic cooperation between the countries of the region was emphasized as a necessary condition. If there was no consensus among the regional elites on the need to break the ties of dependency with the North, the goal of autonomy was almost impossible to achieve.

During the 1990s, with the fall of the Soviet Union, the spread of neoliberal policies and what was seen as the triumph of the unipolar order, the peripheral autonomy school gradually lost weight in academic and political debates in the region and gave way to the paradigm of peripheral realism. This new approach

considered that the region's lack of strategic value made almost any policy of confrontation with the US counterproductive. Given the perceived weakness of the countries in the region, these could not pursue high degrees of autonomy without considerably damaging the welfare of their citizens (Schenoni & Escudé, 2016). Thus, the best strategy for Latin American countries was to align with Washington's interests and avoid any unnecessary confrontation (Escudé, 1992). However, once again, the political, economic, and social changes experienced by most of the countries of the region since the early 2000s, together with a disrupted international order following the September 2001 attacks, challenged this model as the best strategy. In its place, new approaches emerged that took up the idea of autonomy and tried to adjust it to a changing regional and global scenario.

3.2. *Relational autonomy*

Russell and Tokatlian (2003) proposed an updated version of the concept of autonomy, which they called relational autonomy. Their goal was to adapt the notion of autonomy to a new international context characterized by globalization, growing interdependence, and the increasing importance of non-state actors and transnational networks. Recognizing the anachronism of a strategy that put the agency almost exclusively on the power of the state, and that had tended to translate into policies of isolation or direct opposition to the central powers that did little to overcome the problems faced by the region, the authors considered that in the XXI century the autonomy of Latin American countries would be defined by its capacity to have a voice in global discussions. Thus, they defined relational autonomy as the "capacity and willingness of a country to make decisions with others of its own free will and to deal jointly and responsibly with situations and processes occurring within and outside its borders" (Russell & Tokatlian, 2003, 14). Without ignoring the region's subordinate position in the global scenario and the practices of power politics, they presented relational autonomy as the most effective strategy "to reduce power asymmetries and counteract these practices through competent, active, committed and responsible participation in world affairs" (Russell & Tokatlian, 2010, 138).

In practice, relational autonomy could be achieved through three strategic options: i. binding multilateralism; ii. selective collaboration; and iii. limited containment. All three share the same objective, which is the expansion of the degrees of freedom to act independently and in cooperation with others on the international arena. Firstly, binding multilateralism consists of taking advantage of global institutions and multilateral organizations to limit the discretionary use of power and to encourage great powers' compliance with existing rules⁹. Secondly, selective collaboration involves building cooperative ties with major powers "to affect the way they exercise their power and influence and define their interests, transmit information, shape expectations and jointly address common problems" (Russell & Tokatlian, 2010, 141). Finally, limited containment implies the development of regional spaces and instruments for domestic action that reduce or exclude the interference of major powers. This strategy would allow states to expand their degrees of freedom as well as deepen regional cooperation without directly confronting global powers. The "conditions of possibility" for each of these strategies would be determined by both the internal and external context of each particular point in time. It was not necessarily a matter of choosing one strategy, but also of combining them in the most favorable way, based on these conditions and according to the specific domain.

Relational autonomy was proposed as a conceptual basis to think about different policy areas almost two decades ago in a regional and global context very different from the current one. Yet, there are several elements within this theory that can provide us with valuable analytical lenses when considering the adoption and implementation of digital technologies in South America.

First, by framing the discussion in terms of relational autonomy, it allows us to escape the controversy around the relevance of national borders in today's

⁹ The assumption is that institutions influence state behaviors, both constraining the way in which they can make use of their power and legitimizing their policy choices. While major powers are unlikely to submit to the dictates of international institutions, they cannot constantly ignore them without paying increasing costs in terms of credibility and alliances.

globalized world, a point to which, as we have seen in the previous section, it is inevitable to return to when we speak about sovereignty. Drawing on Morin's theory of complex thought (1990), relational autonomy recognizes that autonomy and dependence are not opposites, since "there is no autonomous being or organization that, simultaneously, is not dependent on an external environment (...) at the same time that the agent 'self-determines' itself by distinguishing itself from its environment and thus building its autonomy and individuality, it introduces itself into the external environment, since in isolation it can neither complete nor suffice itself" (Russell & Tokatlian, 2010, 135). Therefore, reflecting on the governance of digital technologies through the lens of relational autonomy does not imply a search for autarchy, nor a denial of the complexity of the digital world and the cross-border nature of many of its elements and actors.

Second, relational autonomy admits the incorporation of new powerful state and non-state actors into the discussion: South American digital autonomy should no longer be thought of only in relation to the US, as the theory was intended at the time, but also to China, and particularly to American and Chinese big tech companies. Although the focus is still mainly on the level of the state, because it is still there that major policies are ultimately defined, attention is paid to the role played by other actors, both upwards - multinational companies, and regional and international organizations - and downwards - civil society and local companies.

Third, relational autonomy sheds light on the fact that one can be legally sovereign, but still have very little autonomy around digital technologies. In February 2021, Australia could have implemented a new legislation requiring Facebook to pay publishers if it hosted their content, but did not because in response to it, the company decided to block Australian users from viewing or sharing news (Morrison, 2021). Given the popularity of the social platform, the government would probably have faced massive public backlash. This was not a threat to Australian sovereignty in the traditional understanding of the notion, but to its capacity to freely decide on legislation for Australians.

Lastly, throughout the last century, the idea of sovereignty – as well as that of autonomy in a more traditional sense – has been used in Southern Cone countries by nationalist governments with dubious democratic credentials to encourage logics of conflict and confrontation with neighboring countries (Russell & Tokatlian, 2010). For this and other reasons, it could be argued that the concept of sovereignty linked to the digital world tends to polarize the debate around these topics, instead of allowing the design of consensual policies. In contrast, few people today would argue against a strategy that seeks to increase the degrees of freedom of action of either a region, a country, or its citizens, which is, in essence, what relational autonomy aims for.

Going back to the definition, thinking about digital transformation in the Southern Cone countries through the lens of relational autonomy would then imply looking for ways to increase the ability and willingness of these countries to make decisions regarding digital technologies of its own free will, as well as to deal collaboratively and responsibly with social, political, and economic phenomena occurring within and outside their borders. What kind of decisions are we talking about? What are the specific circumstances and processes that are taking place within and beyond the Southern Cone? Furthermore, of the three strategies mentioned above, which would be the most appropriate in the current local, regional, and global context? In the second part of this paper, I will delve into these questions.

4. Methodological approach

Building on the three strategies proposed by relational autonomy theory, this research aims to explore the main challenges for achieving digital autonomy in Southern Cone countries, namely Argentina, Brazil, Chile, and Uruguay. The goal is threefold. First, to understand what the state of these discussions is both at a national and a regional level¹⁰. Second, to examine what the main barriers to coordinated action are. Third, to elucidate on what grounds policies towards greater digital autonomy could be developed. To this end, a series of interviews were conducted with actors from civil society, the private sector, and the public sector of the four countries.

The selection of the interviewees was made through previous research in which I tried to elucidate which were the main actors working on the governance of digital technologies in each of the countries. Considering time constraints, a total of 26 individuals and organizations were identified and approached by email, explaining the objectives of the research. With the 18 individuals and organizations that replied positively (*see Table 1*), semi-structured interviews were carried out via Zoom, which lasted an estimated average of half an hour. The questions were modified according to the sector and the specific area of digital technologies in which each interviewee worked. The semi-structured nature of the interviews allowed for greater flexibility: although I had a series of predefined questions, these were adapted according to the direction taken by each interviewee during the conversation and the interest they showed on the various sides of the subject matter. The interviews were recorded with their consent and manually transcribed¹¹. A thematic analysis was then carried out to find common patterns, variances and specificities (Bryman, 2016).

¹⁰ Compared to Europe, where digital sovereignty has been little but increasingly studied by academic research (Pohle and Tiehl, 2020), in South America there are very few works on the subject (see Ávila Pinto, 2018; Ceballos et al., 2020; Becerra & Waisbord, 2021). This could be due, among other reasons, to a lack of academic interest in the area, to an absence of digital policies to be explored, or to the fact that it is a concern that, although latent, has not yet permeated the region.

¹¹ Transcripts are available upon request.

Table 1

Organisation	Sector	Country*	Organisation	Sector	Country*
Access Now	Civil society	Argentina	ILDA	Civil society	Uruguay
Amazon Web Services	Private sector	Argentina	InternetLab	Civil society	Brazil
Autoridade Nacional de Proteção de Dados	Public sector	Brazil	Non-Aligned Tech Movement	Civil society	Argentina
DATA Uruguay	Civil society	Uruguay	O.D.I.A.	Civil society	Argentina
Former Ministry of Industry, Energy and Mining	Public sector	Uruguay	Pontifical Catholic University of Chile	Civil society	Chile
Senate Advisor	Public sector	Chile	Former Access to Public Information Agency	Public sector	Argentina
Former Undersecretary of Telecommunications	Public sector	Chile	Satellologic	Private sector	Argentina
Fundación Vía Libre	Civil society	Argentina	Senate - former Future Challenges Commission	Public sector	Chile
Undersecretariat for Information and Communications Technologies	Public sector	Argentina	Ualá	Private sector	Argentina

**Note.* By country, I refer only to the country of the person interviewed. In many cases, the organizations to which they belong have a presence or provide services in several jurisdictions.

Given the complexity and diversity of perspectives from which the governance of digital technologies can be approached, this study does not attempt to cover all aspects. Rather, it aims to elucidate only some of its dimensions and their development at the regional level from the lens of relational autonomy. These dimensions were not defined in advance; instead, the conversation was left open for the actors interviewed to address the areas that were most important to them.

5. Findings and discussion

5.1. Positions regarding digital sovereignty¹²

All the interviewees were able to put forward their views on the concept of digital sovereignty. Still, several of them asked to specify what I meant by this notion and stated that they were not familiar with it or had not previously worked with it. This suggests, on the one hand, that digital sovereignty is also a “fuzzy” concept (Elms, 2021) at the regional level, and on the other, that it is a discussion that clearly is not as widespread in the Southern Cone as in other parts of the world. The main policy areas with which the concept was immediately associated had to do with equal access to digital technologies, a greater control over data flows, data storage and data processing, the safeguarding of citizens’ personal data, and the development and deployment of free software¹³.

A first glance at the interviews could indicate two positions regarding digital sovereignty that echo the debate identified in the first part of this paper. On the one hand, there are those who believe that it is a valuable concept. According to one of the respondents, sovereignty has to do with the way in which a group of people governs itself, and today the different forms of government are very much crossed by digital technologies. This first group assumes that states continue to be the fundamental basis on which digital policies are structured.

“Sometimes we forget this last factor, which is that nation states are very much alive and kicking, as evidenced when they close the borders in the middle of a pandemic.” (Personal communication¹⁴, March 2022)

¹²Although this work proposes thinking in terms of digital autonomy, the concept used in the interviews was that of digital sovereignty, since being a more widely known concept, it allowed the interviewer to avoid having to give further conceptual precisions that could bias the answers.

¹³There are other highly important dimensions of digital sovereignty or autonomy, such as surveillance technologies or cryptocurrencies, which were raised by some interviewees, but for reasons of time and space were left out of the analysis.

¹⁴Anonymity was guaranteed, more information about the quotations upon request.

Another group of interviewees, on the other hand, considers that speaking about digital sovereignty is an attempt to replicate old structures in the digital world. Yet, a deeper analysis would suggest an overarching agreement between the eighteen interviewees: the need to reduce South American countries' dependence on the provision of digital services by foreign companies, as well as to develop adequate frameworks to protect citizens' personal data.

Starting from this basis, the major point of disagreement had to do with data localization policies. In general terms, the respondents in favor of these requirements tended to defend a greater role of the state regarding the digital world. Still, most of them agreed on the need to differentiate between categories of data and to identify which sensitive information needs to be safeguarded. In this sense, one of the interviewees stated that since most of the state's data is or should be public, as long as there is a local copy, whether it is hosted within national borders or not would not make a difference in strategic terms. On the other hand, those who expressed their disagreement with data localization argued that these measures went against the free flow of information across borders and had a direct impact on the economy, something that the countries in the region were not able to afford. This same group of respondents also expressed doubts regarding the development of a public cloud and the imposition of mandatory criteria for certain data to be hosted in it.

"It seems to me that when talking about digital sovereignty, if the idea is that there can be no processing of personal data, or rather that there should be an obligation for states to impose that the data of nationals of that country be housed in data centers within that country is first absurd, and second dangerous. There are countries in which the real advantage is that people's data is not hosted in that country."

(Personal communication, March 2022)

Several of the respondents argued that they distrusted greater state control over circulating data and called attention to the fact that digital sovereignty may be used as an excuse to gain greater control over populations. In some cases where concern was expressed about the fact that a large amount of

sensitive and personal data would be in the hands of private companies, it was also noted that they did not feel reassured by the idea of it coming under state control. Furthermore, two of the interviewees stated that they would prefer that such data be in the hands of large tech companies somewhere in the US, rather than in their own country.

Regarding privacy, the recurring argument was that as long as the data was properly encrypted, it made no difference where it was stored. Against this point, one interviewee pointed out how misleading the encryption argument could sometimes be. As an example, he argued that although WhatsApp offers an end-to-end encrypted service – which means that it does not have access to the content of messages – it does have access to users’ metadata, such as their location or connection duration and frequency (Rastogi & Hendler, 2017). This is the type of information that can be later exploited by Meta, WhatsApp’s parent organization, to understand users’ behavior and social interactions to better target them.

Beyond privacy, two interviewees noted that debates around the value of data also have a very important aspect to do with security, and how in a potential conflict context, digital platforms can become a strategic resource:

“In the end you always end up on a server in another country, which is covered by that other country’s legislation. It’s not just about Amazon spying on me. It’s not just a privacy issue, which of course with encryption techniques can be solved. It’s a security issue, what happens if they cut my cable, if they disconnect me for some reason. (...) How do I ensure the continuity of my services? It’s a discussion that seems absurd, but at the end of the day it’s not. What happens is that they put a lot of layers of abstraction on top with which they convinced you that you live in a world that is abstract and that the data is nowhere.” (Personal communication, March 2022)

The analysis of the different positions suggests that there is a general understanding that discussions around control over cross-border data flows are not just technical, but also, and more importantly, political and economic. At the same time, there seems to be little clarity on technical and legal aspects that are

also fundamental to the discussion, such as jurisdiction over data from one country that is hosted in third countries. Perhaps because of this lack of clarity and the blurred lines that emerge when the digital and analog worlds intersect, four interviewees advised bringing the concept of digital sovereignty down to the level of practice, and analyzing which policies are being implemented and which are not before adopting any position on the matter. According to one of them, it was possible to identify a political discourse linked to sovereignty which often did not translate into concrete measures and policies.

5.2. *Main identified barriers*

When identifying the main barriers to better protecting state and citizens from the negative impacts of digital technologies and reduce reliance on a few foreign companies, the lack of adequate regulatory frameworks emerged as the most important one. In some cases, it was mentioned that even if the framework existed, it was often outdated or not properly enforced. One of the interviewees argued in relation to the devaluation of the Argentine currency and its implications on personal data protection legislation:

“The amount of the fines under Argentine law is a derisory amount for any company, it is more convenient for the company to break the law and pay the fine than to adapt its structures so as not to infringe it.”

(Personal communication, March 2022)

A second salient theme was poor technical expertise at the state level. Different explanations were put forward for this. First, several interviewees pointed out to a lack of real interest in the subject on the part of the political elites, which still consider issues related to digital technologies as part of a technical discussion and not as a strategic topic. Second, they indicated that their countries usually do not have the economic means to compete with the private sector in these areas and attract better human resources. Third, they mentioned that even when there were people qualified to understand the complexity of the challenges

and implement good policies, many times these people were in intermediate positions and had superiors who did not have knowledge on the subject and were appointed because of their political affiliation. In this line, several of the respondents argued that the technical expertise at the regional level does exist, and that the problem is that it is often not consulted or listened to. On top of all these problems, there is a strong presence of corporate lobbies, which hinders good regulation:

“In general we are outdated and the regulator does not understand what they are doing (...) even when you have regulators that want to do things better, because they are informed, they know what to do, or because they are copying what exists in other jurisdictions, you have the problem of the lobby that is not regulated or is poorly regulated, and they are co-opted by those interests.”

(Personal communication, March 2022)

The absence of a comprehensive digital strategy, of a public policy sustained over time with a clear objective, as well as the fact that there is no specific office in each country to lead on these subjects, also makes it difficult to compare policies between neighboring countries and to coordinate at the regional level. Although there are regional spaces in which there is a certain degree of technical cooperation, this often does not translate to high political levels, which impedes the harmonization of digital strategies. Moreover, cooperation in regional organizations is often constrained by the high turnover of national staff which is subject to changes in government.

The problems identified thus far at the state level reflect, and at the same time impact on, what is happening within the citizenry. Most of the interviewees agreed that in general, citizens were largely unaware of their digital rights, as well as of the risks posed by emerging technologies and the concentrated power of large technology companies. One interviewee suggested that although in recent years the level of awareness had increased, many people did not care about their digital rights because the advantages the digital platforms offered

were deemed to be much more important. In contrast, another respondent argued that it was not the case that citizens did not care about their data. Instead, the problem was a lack of confidence that public institutions would be able to enforce their rights. Thus, a low level of knowledge, concern, or trust among the citizenry on the one hand, and the lack of real interest in the subject at the level of public administrations on the other, would feed each other and prevent the development of a comprehensive view of the characteristics, challenges, and opportunities of digital transformation.

5.3. *Variances within the region*

Although the diagnosis is more or less similar for all Southern Cone countries, there are some that are more advanced than others. Brazil appears to be the country where issues related to data sovereignty, cybersecurity and the protection of digital rights have been discussed the most in the last decade¹⁵. In 2014, the enactment of the *Marco Civil da Internet* set an important precedent both regionally and globally in terms of the protection of users' rights in the digital sphere (Canineu & Donahoe, 2014). Four years later, it passed the *Lei Geral de Proteção de Dados* (or LGPD), the Brazilian version of the European General Data Protection Regulation (GDPR). One of the Brazilian organizations pointed out that it had been a very important step that had made it possible to bring the issue of personal data protection into the public debate, but that the second step, that of implementation, was proving much more difficult. At the same time, Brazil seems to be facing other very important challenges regarding the implementation of digital technologies. An issue that is beyond the scope of this paper but for which interviewees also expressed their concern was the trend towards the abuse or misuse of digital technologies, particularly by law enforcement agencies¹⁶.

¹⁵This would support Becerra and Waisbord's (2021) thesis that digital sovereignty issues are a concern of countries that have global geopolitical ambitions.

¹⁶The deployment of facial recognition systems in police forces was presented as one of the main challenges faced by Brazilian citizens regarding the deployment of emerging technologies.

Another country that interviewees pointed out as being at the forefront of digital transformation is Uruguay. Four of them stated that it had made steady progress in some very important areas, such as the deployment of free and open-source software in public institutions. In contrast, when it comes to Argentina, one of the organizations interviewed voiced their concern about the lack of progress in the use of free and open-source software in the public sector. One of the areas of greatest alarm was public education, where although progress has been made, proprietary software continues to be used. On the same line, another topic that was presented as particularly sensitive for Argentina was the increasing number of data leaks¹⁷.

Regarding Chile, while interviewees agreed that the ongoing process of political transformation has dominated all public debate in recent years, and thus these topics have not been given much attention, they also suggested that it could lead to cutting-edge legislation that incorporates an important technological backbone. On a closely related topic, in 2020, Chile became the first country in the world to incorporate the protection of neuro-rights into its Constitution. Furthermore, according to one interviewee, there would be much potential for cooperation on digital technologies between Chile and Argentina. Yet, the differences between the political dynamics in each country would seem to make a regional harmonization unlikely in the short term.

5.4. *Strategies towards digital autonomy*

Based on the different opinions collected regarding the major challenges facing the South American region in general, and each country in particular, it is possible to identify a number of broad policy guidelines that would help to move towards digital autonomy. This is intended as a recommendation exercise and

¹⁷According to several of the respondents, the outlook is extremely alarming: in October 2021, in what amounted to the largest data breach in Argentine history, a user managed to access the database of the National Registry of Persons and disclose sensitive data of 60,000 Argentine citizens (Brodersen & Blanco, 2021).

does not imply that the region is close to that goal, much less that it is a goal at present. Digital autonomy, as understood in this paper, should not be seen from a binary perspective – a region, country, or community either has or does not have digital autonomy – but rather as a continuum in which there are opportunities to develop policies that allow moving towards a common goal.

Most of the recommendations drawn from the interviews have to do with domestic capacity building. In this sense, the strategy that seems to prevail regarding digital technologies is that of limited containment, that is, the creation or expansion of regional spaces and instruments for local action that reduce or exclude the interference of major powers. In *Table 2* the main recommendations drawn from the interviews were summarized and placed under each of their respective strategies.

Table 2

	Limited containment	Selective collaboration	Binding multilateralism
<i>Country level</i>	Investment on the development of critical infrastructure	Increased collaboration and coordination with the EU in the development and enforcement of regulatory frameworks	Increased South American involvement in key multilateral institutions
	Advancement of regulatory frameworks to protect citizens and to foster a more diverse local digital environment	Agreements with tech companies to cover those areas where the state and the local private sector cannot offer digital goods and services	
	Greater investment in human capacities within the public sector		
	Increased efforts to promote greater awareness among the citizenry		
	Further spaces for dialogue and exchange between all stakeholders		
<i>Regional level</i>	Greater coordination on legal frameworks		
	Development of an in-depth dialogue on the governance of digital technologies		

*Source: own elaboration.

The need for a greater state role in the development of a comprehensive policy regarding digital technologies was a common denominator in almost all the interviews. A first fundamental point had to do with the development of critical infrastructure, or the fostering of better governance of the existing one. Secondly, more efforts should be made to develop and implement good regulatory frameworks to protect citizens, but also to encourage innovation and competition at the local level, to deconcentrate data monopolies, and to allow the emergence of many different alternatives. On this point, one of the interviewees argued that the lack of good regulatory frameworks prevented the emergence of companies competing with proposals more in line with local culture.

“There are ways in which we communicate among people from other cultures, which may require or benefit from a different design that is not going to appear as long as a company like WhatsApp is dominant in the market.”

(Personal communication, April 2022)

Providing the citizen with the possibility of choosing from a diversity of technical options was also a fundamental point. The goal should not only be regulating large tech companies, but also smaller players that tend to adopt the same business models and often go unnoticed.

“Why does Facebook have to be the one that contains the social graph of my relationships with all my friends and at the same time be the same entity that presents me with information and orders it for me, and the one that engages in content moderation and executes a function of a court of law? Those three functions could be unbundled into three different services, if they were interoperable. That is political will and legislation. And at the same time also technological development that has to be stimulated and paid for. Changing tyrants is never a good option.”

(Personal communication, March 2020)

For the citizens to be able to choose, there must be greater awareness of the advantages and risks posed by digital technologies. This would generate a virtuous circle in which a more aware citizenry would demand higher security standards from companies and new and better policies from their governments, and in turn these new policies and legal frameworks would enrich public debate

and promote a greater understanding of the value of data and digital technologies in general.

Along the same lines, initiatives such as the development of a public cloud would seem to be welcome, as long as they are aimed at offering citizens more options, and not at imposing a single technological option. Any improvement in technological developments should go hand in hand with another aspect on which all interviewees agreed: the need for greater investment in human capacities within the public sector, promoting much better wages but also facilitating training in a sector that is constantly evolving. Public officials could also benefit from the development of spaces for dialogue and exchange with civil society organizations and academia where there is a lot of untapped expertise on these topics. These new opportunities for dialogue should be encouraged within each country, but also at the regional level. Indeed, two of the organizations consulted pointed to the need for greater regional coordination, which would not be unthinkable even in a scenario of little integration.

“When we talk about achieving IT sovereignty, we talk about being able to make our own decisions. Own decisions are limited by scale, and the scale is going to be Latin American, or it is not going to be.” (Personal communication, March 2022)

Only one of the interviewees mentioned the Southern Common Market (MERCOSUR) as a venue in which there were conversations around these issues. Although MERCOSUR is currently facing a scenario of disintegration rather than integration (Malacalza and Tokatlian, 2021), it was not completely ruled out that in the future, the union could provide a space from which to promote a regional conversation of greater tenor around these issues. Other regional organizations that were identified as facilitating incipient conversations around various dimensions of the digital transformation included the Inter-American Development Bank (IDB), the Development Bank of Latin America (CAF), and the Economic Commission for Latin America and the Caribbean (ECLAC). These are all spaces that could be better used for the exchange of knowledge and capabilities, for greater coordination, and more broadly, for the development of

an in-depth dialogue on the governance of digital technologies. In the quest for greater digital autonomy, one of the respondents recommended avoiding the “big titles” or ventures, and going step by step, creating small spaces of containment.

The second strategy under which some of the recommendations for moving towards greater digital autonomy could be placed is that of selective collaboration. Selective collaboration can occur bilaterally or regionally and entails the development of cooperative ties with other powerful actors “to cope jointly with common problems, reduce uncertainties, and avoid mutual errors of perception” (Russell & Tokatlian, 2011, 140-141).

With some exceptions, there is a favorable perception towards the adoption of regulatory frameworks that accompany European legal developments, both in terms of personal data protection – GDPR – and the regulation of big tech platforms – Digital Services Act (DSA) and Digital Markets Act (DMA). According to the respondents, this could be of benefit to both regions: on the one hand, Europe could extend its leadership in terms of standard-setting outside the region and profit from increased data transfer and hosting in its territory; on the other hand, by updating its legislative provisions, Southern Cone countries could also gain from increased data transfer to the region and a redirection of much of its data that is currently hosted in places without adequate protection to more secure jurisdictions. Having a relatively homogeneous legislation with the EU would also potentially increase users’ trust in the exercise of their digital rights, since the same rules would apply in either territory. One of the key areas identified by the interviewees from which South America as a region could draw valuable elements is the European interoperability strategy.

Still, respondents also emphasized the importance of paying attention to local specificities and adapting frameworks based on implementation capabilities to avoid a stunted transfer of policies, or, in the words of one of the interviewees,

the creation of a “Frankenstein”. European policy and legal advances were the result of many years of broad dialogue on these issues, a relatively aware citizenry, and the involvement of all stakeholders. Attempting to replicate the regulatory frameworks without first having one’s own broad dialogues, would run a very high risk of resulting in unenforceable legislation.

A second actor with whom a selective collaboration could be established are large tech companies. Even though this point may sound contrary to the quest for digital autonomy, Southern Cone countries are far from being technologically self-sufficient. Any policy seeking to impose the use of exclusively local technological solutions on citizens and the private sector would probably result in a significant technological gap in relation to other parts of the world, and with a population upset at not being able to access other options. That is why, at least in the short and medium term, cooperation links will inevitably have to be established. This does not mean that Amazon or Google can operate within the region without any kind of control and accountability, nor that the public sector makes use of their services indiscriminately; rather, it implies a prior exercise of deep, sincere, and responsible evaluation of those areas that the state or local companies cannot cover at present together with the development of regulatory frameworks that determine what these companies can and cannot do. Given the size and power of these companies, the bargaining power that countries will have to impose legislation according to their interests will be determined by the size of their markets. In this sense, the more the countries of the region coordinate their policies, the more likely it will be that their regulations will be complied with.

All in all, binding multilateralism appears to be the least relevant strategy in the current context. Indeed, very few interviewees mentioned instances of global cooperation on these topics as possible spaces in which Southern Cone countries could have a greater voice and bargaining power. Furthermore, one of the interviewees referred to an ongoing global competition among multilateral organizations to represent the venue where these discussions should take place.

This is arguably due to the growing trend towards fragmentation of digital technologies governance models and the increasing erosion of the binding and symbolic power of the multilateral bodies that could develop a global governance for these technologies. Still, the fact that multilateral organizations are not playing an important role in the development of global frameworks for the governance of digital technologies does not imply that these spaces do not exist or that they will not have a greater importance in the future. As history has shown on several occasions, the geopolitical context can evolve rapidly. Therefore, Southern Cone countries should not underestimate the multilateral spaces where these discussions are taking place – such as UNESCO, the Internet Governance Forum (IGF), the World Economic Forum (WEF), and the OECD – and seek to adopt a proactive role in the development of global frameworks that set a more favorable course for digital transformation from the lens of developing countries.

6. Looking forward

So, can we expect a brighter future? The answer to this question will clearly depend on the expectations of each reader. As the interviews conducted during this research made clear, the views on the nature and impact of digital technologies, on the role of the state and tech giants, as well as on the policies that should be followed, are far from being uniform within the Southern Cone. Still, it seems possible to outline some intermediate paths, around which there seems to be general agreements at the regional level, that would help to advance towards greater digital autonomy. In a context of international fragmentation around the governance of digital technologies and increasing technological competition between the US and China – amid which the region has been caught¹⁸ (Mearsheimer, 2014; Russell, 2021) –, the strategy that appears to be the most appropriate for the coming years is that of limited containment. This involves the development of regional spaces and instruments for domestic action that reduce or exclude the interference of major powers. Today, particularly in this area, major powers are the US, China, and above all, these countries' big tech companies.

South American countries may choose whether to pursue this strategy separately or to coordinate their digital policies to move towards greater autonomy at the regional level. The current scenario of regional disintegration – understood as the “decline of a way of designing and implementing common and shared policies on a wide range of issues” (Malacalza & Tokatlian, 2021) – would seem to work against the latter option. According to Walt (1997), one of the reasons why alliances fail is because of changes in the perceptions of threat. These changes occur when “as a result of a rearrangement of the existing order or a transition of world power, members of an organization decide to give

¹⁸ China's growing presence and influence in Latin America has led Washington to observe with great concern what it sees as an incursion of an extra-regional actor in its historical area of influence. US officials have not hesitated to warn Latin American countries about the implications of China's growing investment in the region, particularly in the field of 5G (Guerra, 2019; Pérez Izquierdo, 2019). According to Russell (2021), Latin America's margins of autonomy will depend to a large extent on the degree of tension or flexibility that the rivalry between the US and China acquires.

individual responses to global constraints and opportunities” (Malacalza & Tokatlian, 2021). It is worth asking, however, whether these changes could act in the opposite direction: would it be possible to envisage a future regional scenario in which Southern Cone countries, faced with the advance of digital technologies, the overwhelming expansion of a few extra-regional tech companies’ power, and the deepening of the US-China competition, decide to coordinate their internal and external digital policies? A change in the perceptions of threat could thus give rise to a new common interest – digital autonomy – which could underpin a regional strategy of limited containment.

Recognizing the limitations of a research based on a small number of interviews, this work has not sought to provide specific policy recommendations, an effort which would have to provide a much more detailed account of all the relevant variables. Rather, it aimed to contribute to the discussion around the governance of digital technologies in the Southern Cone from an international relations perspective, and to outline possible ways forward in an area that is extremely complex but which should not be limited to a technical approach. In their work on the absence of cybernationalism in Latin America, Becerra and Waisbord (2021) concluded that “only countries and regions that meet certain conditions, such as market size, geopolitical power, and/or strong developmentalist policies, may be able to pursue the paths of media nationalism and digital sovereignty” (p. 77). This work has tried, from a perhaps ambitious but not naïve perspective, to challenge this approach by showing that Southern Cone countries have indeed developed policies in recent history aimed explicitly or implicitly at greater digital autonomy, and that there is still ample ground on which to keep building. Democracy has been defined as “a political system that does not definitely close off the possibilities for reflection and change of institutionalised realities” (Helmut, 1994, 112). In South America, despite the many barriers, the road to digital autonomy remains open.

REFERENCES

- Aguerre, C., & Tarullo, R. (2021). Unravelling resistance: Data activism configurations in Latin American civil society. *Palabra Clave*, 24(3), 5.
- Autolitano, S., & Pawlowska, A. (2021). *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study*. Istituto Affari Internazionali (IAI).
<https://www.jstor.org/stable/resrep30940>
- Brodersen, J. (2021, October 23). Filtración del Renaper: Difunden datos sensibles de 60.000 argentinos y piden cerca de 17 mil dólares por todos los DNI. *Clarín*.
https://www.clarin.com/tecnologia/filtracion-renaper-difunden-datos-sensibles-60-000-argentinos-piden-cerca-17-mil-dolares-dni_0_2eE_kXXBo.html
- Broeders, D., & Berg, B. van den. (2020). *Governing Cyberspace: Behavior, Power and Diplomacy*. Rowman & Littlefield.
- Bryman, A. (2016). *Social Research Methods*. Oxford University Press.
- Burrows, M., Mueller-Kaler, J., Oksanen, K., & Piironen, O. (2021). *Unpacking the geopolitics of technology*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/unpacking-the-geopolitics-of-technology/>
- Burwell, F., & Propp, K. (2020). *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?* Atlantic Council.
<https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>
- Ceballos, L. D., Maisonnave, M. A., & Londoño, C. R. B. (2020). Soberanía tecnológica digital en Latinoamérica. *Propuestas para el Desarrollo*, IV, 151–167.
- Collini, L., Rabuel, L., & Carlberg, M. (2021). *Study on mapping data flows | Shaping Europe's digital future*. <https://digital-strategy.ec.europa.eu/es/node/10696>
- Colomina, C. (2021). *Europe offers a third way in the technological transformation*. CIDOB.
http://www.cidob.org/es/publicaciones/serie_de_publicacion/notes_internacionales_cidob/263/europe_offers_a_third_way_in_the_technological_transformation
- Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, 20(4), 336–349.
<https://doi.org/10.1177/1527476418796632>
- Couture, S., & Toupin, S. (2018). *What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty?* (SSRN Scholarly Paper ID 3107272). Social Science Research Network. <https://doi.org/10.2139/ssrn.3107272>
- Crawford, K., & Joler, V. (2018). *Anatomy of an AI System*. Anatomy of an AI System.
<http://www.anatomyof.ai>

Discours du Président Emmanuel Macron sur la stratégie de défense et de dissuasion devant les stagiaires de la 27ème promotion de l'école de guerre. (2020, February 7). *elysee.fr*.
<https://www.elysee.fr/emmanuel-macron/2020/02/07/discours-du-president-emmanuel-macron-sur-la-strategie-de-defense-et-de-dissuasion-devant-les-stagiaires-de-la-27eme-promotion-de-lecole-de-guerre>

Echos, L. (2011, August 30). De la souveraineté en général et de la souveraineté numérique en particulier. *lesechos.fr*.
http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

Elms, D. (2021). *Digital Sovereignty: Protectionism or autonomy?* Hinrich Foundation.
<https://www.hinrichfoundation.com/research/wp/digital/digital-sovereignty-protectionism-or-autonomy/>

Emmott, R. (2014, February 24). Brazil, Europe plan undersea cable to skirt U.S. spying. *Reuters*. <https://www.reuters.com/article/us-eu-brazil-idUSBREA1N0PL20140224>

Fibre-optic cables: The present and future of digital technology. (2021, August 31). *EllaLink*.
<https://ella.link/2021/08/31/fibre-optic-cables-future-of-digital-technology/>

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33(3), 369–378.
<https://doi.org/10.1007/s13347-020-00423-6>

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiinaud, L., Winkler, J., & Zanin, C. (2022). Contested Spatialities of Digital Sovereignty. *Geopolitics*, 0(0), 1–40.
<https://doi.org/10.1080/14650045.2022.2050070>

Guerra, I. (2019, April 12). Mike Pompeo advierte a Chile sobre China y Huawei: "Esa infraestructura presenta riesgos a los ciudadanos de tu país". *Emol*.
<https://www.emol.com/noticias/Nacional/2019/04/12/944543/Mike-Pompeo-advierte-a-Chile-sobre-China-y-Huawei-Esa-infraestructura-presenta-riesgos-a-los-ciudadanos-de-tu-pais.html>

Habermas, J. (2001). *The Postnational Constellation: Political Essays*. MIT Press.

Hache, A. (Ed.). (2014). *Soberanía tecnológica* (Ritimo).
<https://www.ritimo.org/IMG/pdf/dossier-st1-es.pdf>

Hobbs, C. (2020, April 8). The EU as a digital regulatory superpower: Implications for the United States – European Council on Foreign Relations. *ECFR*.
https://ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u/

Hobbs, C., & Torreblanca, J. I. (Eds.). (2020). *La soberanía digital de Europa | varios autores*. Los Libros de la Catarata. <http://www.marcialpons.es/libros/la-soberania-digital-de-europa/9788413521268/>

- Innerarity, D. (2021). *European digital sovereignty* [Working Paper]. Institute of European Democrats (IED). <https://cadmus.eui.eu/handle/1814/73437>
- Jaguaribe, H. (1979). Autonomía periférica y hegemonía céntrica. *Estudios Internacionales*, 12(46), 91–130.
- Khazan, O. (2013, July 16). The Creepy, Long-Standing Practice of Undersea Cable Tapping. *The Atlantic*.
<https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>
- Krasner, S. D. (2001). Sovereignty. *Foreign Policy*, 122, 20–29.
<https://doi.org/10.2307/3183223>
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. <https://doi.org/10.1177/0306396818823172>
- Linklater, A. (1998). *The Transformation of Political Community: Ethical Foundations of the Post-Westphalian Era*. Univ of South Carolina Press.
- Mearsheimer, J. J. (2014). Can China Rise Peacefully? *The National Interest*.
<https://nationalinterest.org/commentary/can-china-rise-peacefully-10204>
- Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond Data Universalism. *Television & New Media*, 20(4), 319–335. <https://doi.org/10.1177/1527476419837739>
- Mirrlees, T. (2020). *Getting at Gafam's "Power" in Society: A Structural-Relational Framework*. HELIOTROPE. <https://www.heliotropejournal.net/helio/gafams-power-in-society>
- Morin, E. (1990). *Introducción al pensamiento complejo*. Gedisa.
https://norberto2016.files.wordpress.com/2016/10/morinedgar_introduccion-al-pensamiento-complejo_parte1.pdf
- Morrison, S. (2021, February 18). Why Facebook reversed its news ban in Australia. *Vox*. <https://www.vox.com/recode/22287971/australia-facebook-news-ban-google-money>
- Mueller, M. L. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, 22(4), 779–801. <https://doi.org/10.1093/isr/viz044>
- OECD *Internet Economy Outlook*. (2012). OCDE.
<https://www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm>
- O'hara, K., & Hall, W. (2018, December 7). *Four internets: The geopolitics of digital governance* [Monograph]. The Centre for International Governance Innovation (CIGI)/Chatham House. <https://eprints.soton.ac.uk/427838/>
- Pérez Izquierdo, L. (2019, July 19). Contundente respaldo de Mike Pompeo al presidente Macri: "Ha tomado las decisiones correctas". *Infobae*.

<https://www.infobae.com/politica/2019/07/19/contundente-respaldo-de-mike-pompeo-al-presidente-macri-ha-tomado-las-decisiones-correctas/>

Pohle, J. (2020). *Digital sovereignty. A new key concept of digital policy in Germany and Europe*. Konrad-Adenauer-Stiftung. <https://www.kas.de/en/single-title/-/content/digital-sovereignty>

Rastogi, N., & Hendler, J. (2017). *WhatsApp security and role of metadata in preserving privacy*.

Russell, R. (2021). Latinoamérica ante la competencia entre China y Estados Unidos. *Foreign affairs: Latinoamérica*, 21(4), 6–9.

Russell, R., & Tokatlian, J. G. (2011). Beyond Orthodoxy: Asserting Latin America's New Strategic Options Toward the United States. *Latin American Politics and Society*, 53(4), 127–146. <https://doi.org/10.1111/j.1548-2456.2011.00136.x>

Sahuquillo, M. R. (2019, April 16). Rusia aprueba la ley que refuerza su capacidad de censura en Internet. *El País*.

https://elpais.com/internacional/2019/04/16/actualidad/1555427376_009178.html

Schenoni, L., & Escudé, C. (2016). Peripheral Realism Revisited. *Revista Brasileira de Política Internacional*, 59. <https://doi.org/10.1590/0034-7329201600102>

Segal, A. (2021, July 7). *The Coming Tech Cold War With China*.

<https://www.foreignaffairs.com/articles/north-america/2020-09-09/coming-tech-cold-war-china>

Shaping Europe's digital future: Op-ed by Ursula von der Leyen, President of the European Commission. (2020). *European Commission - European Commission*.

https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260

Siebert, Z. (2021). *Digital Sovereignty – The EU in a Contest for Influence and Leadership*. Heinrich-Böll-Stiftung. <https://eu.boell.org/en/2021/02/15/digital-sovereignty-eu-contest-influence-and-leadership>

The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield, (Court of Justice of the European Union 2020). <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf>

Tiezzi, S. (n.d.). *China Vows No Compromise on 'Cyber Sovereignty.'* Retrieved April 19, 2022, from <https://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty/>

Tocci, N. (2021). *European Strategic Autonomy: What It Is, Why We Need It, How to Achieve It* [Text]. IAI Istituto Affari Internazionali.

<https://www.iai.it/en/pubblicazioni/european-strategic-autonomy-what-it-why-we-need-it-how-achieve-it>

Together for Europe's recovery – Programme for Germany's Presidency of the Council of the European Union. (2020). Bundesregierung.

<https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf>

Tokatlian, J. G. (2022, February 8). Argentina y un triángulo autonómico. *Clarín*. https://www.clarin.com/opinion/argentina-triangulo-autonomico_0_x76mKp4wnh.html

Tokatlian, J. G., & Malacalza, B. (2021, July 25). ¿Es posible la desintegración del Mercosur? *elDiarioAR.com*. https://www.eldiarioar.com/opinion/posible-desintegracion-mercosur_129_8162296.html

Treré, E., & Milan, S. (2021). Perspectivas latinoamericanas sobre la datificación y la inteligencia artificial: Tradiciones, intervenciones y posibilidades. *Palabra Clave*, 24(3), e2431–e2431. <https://doi.org/10.5294/pacla.2021.24.3.1>

van Lindert, T., & van Troost, L. (Eds.). (2014). *Shifting Power and Human Rights Diplomacy*. Amnesty International Netherlands.

Walt, S. M. (2021). Big Tech Won't Remake the Global Order. *Foreign Policy*. <https://foreignpolicy.com/2021/11/08/big-tech-wont-remake-the-global-order/>

What one idea will define 2022? (2021, December 28). *POLITICO*. <https://www.politico.eu/article/what-one-idea-will-define-2022/>

Wickham Heath Consulting. (2018). *Cross-Border Data Flows. Realising benefits and removing barriers*. GSMA. https://www.gsma.com/latinamerica/wp-content/uploads/2019/07/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf

World Employment and Social Outlook 2021: The role of digital labour platforms in transforming the world of work. (2021). International Labour Organization. <https://www.ilo.org/global/research/global-reports/weso/trends2021/lang--en/index.htm>