Shaping a Data Commoning Polity: Prospects and Challenges of a European Digital Sovereignty

Stefano Calzati(✉)

Delft University of Technology, 2626BZ Delft, The Netherlands
s.calzati@tudelft.nl

Abstract. The concept of "digital sovereignty" has gained momentum due to the emergence of a multipolar geopolitical scenario based upon different visions of today's digital society. In this scenario, the United States, China, and the European Union are major players, each pursuing their understanding of digital sovereignty and their approach to digital transformation. The EU conceives of digital sovereignty as technological autonomy from other competitors, and to achieve this it has carved for itself the role of international regulator. De facto, however, the EU enacts an individual-centric and economic-driven digital strategy that hinders the possibility of a fully-fledged European digital sovereignty. Notably, the concept fails to embed the collective-level dimension proper to sovereignty as such. To tackle this, the paper explores data commoning as the basis for shaping a well-formed European polity, key to its digital sovereignty.

Keywords: digital sovereignty · European Union · data commons

1 Introduction

In contemporary political theory, the concept of sovereignty is one of the most debated, being regarded as a contested concept that, at once, has undergone deep changes in meaning – to the point of eroding its epistemological relevance (Agnew 1999) – and one which remains a pivotal feature of the contemporary geopolitical landscape (Werner & De Wilde 2001). An operational definition for the present paper considers sovereignty as "a process in which a group of people within a defined territory is moulded into an orderly cohesion through the establishment of a governing authority that can be differentiated from society and which is able to exercise an absolute political power" (Loughlin 2018). This definition is useful – as we shall see – for two reasons: on the one hand, it identifies the key attributes of sovereignty, notably: territory, authority/power, and community; on the other hand, by departing from a normative (Westphalian) understanding of the term, it stresses the procedural nature of sovereignty as an emergent feature of/within any polity. Based on this premise, the paper explores 1) what does the European Union mean

Published by Springer Nature Switzerland AG 2023
N. Edelmann et al. (Eds.): ePart 2023, LNCS 14153, pp. 151–166, 2023.
https://doi.org/10.1007/978-3-031-41617-0_10

with sovereignty in the context of digital transformation[1]? 2) How does the concept of a sovereign digital transformation impact on the achievement of the EU's digital strategy?

In tackling the first question, the paper follows up on the "linguistic turn" in political theory, whereby concepts once considered as nominally self-sufficient, have been unveiled to be socially constructed, thus depending on pragmatic use for their own validation. "Meaning", then, stands here not much for a dictionary-like definition, but for how the concept is adopted in official documents – EU's policy documents, directives, and regulations – and with which consequences. Concerning the second question, the goal is to investigate the extent to which the meaning of digital sovereignty adopted by the EU hinders and/or favors the pursuing of its digital agenda, based on a strategy that seeks a balance between individual fundamental rights and economic competitiveness, social inclusiveness, and environmental sustainability (von der Leyen 2020).

To do so, a critical review is conducted of latest policy-orienting documents and pieces of legislation published by the EU as part of its digital strategy. According to Grant and Booth (2009), a critical review is a method that delivers "analysis and conceptual innovation" for future informed research and practice. Hence, the present critical review is not exhaustive in scope, but rather identifies (discursive) patterns which then establish, de facto, the way to follow when it comes to governing the digital transformation within the EU. Since the analysis will highlight a discrepancy between the EU's digital strategy and digital sovereignty, the paper will advance some suggestions on how the EU might purse a more coherent sovereign digital strategy. As a note, the paper is conceptual in nature and further testing of its key tenets is needed.

The paper is divided in five sections: Sect. 2 provides an overview on sovereignty as a contested concept in political theory; Sect. 3 explores the concept of digital sovereignty with a focus on the EU in relation to its main technological competitors; Sect. 4 is concerned with how this conceptualization of digital sovereignty relates to the EU's digital strategy, highlighting a potential misalignment; Sect. 5 outlines key conceptual tenets to enact a fully-fledge European digital sovereignty; Sect. 6 summaries the key points and points towards further research.

2 Sovereignty

Based on a normative Westphalian understanding, the nation-state has been traditionally the privileged locus of sovereignty. In fact, in the nation-state we witness the overlap of the triad territory, authority/power, and community, which is at the core of a legal and political characterization of sovereignty. However, especially since the second half of the 20th century, the endowment of the nation-state with such sovereign legitimacy has gotten increasingly contested along at least four axes: 1) the misalignment between sovereignty *de iure* and *de facto*; 2) the extension of sovereignty to supra- and sub-national dimensions; 3) the clash between the state and private actors; 4) the consolidation of an infrastructural global network cutting physical-virtual borders. While these axes are deeply intertwined, they are disentangled here for analytical purposes.

[1] Here "digital transformation" refers to the sociotechnical effects of digitalization, intended as the translation of physical reality into a set of 0s and 1s, through data-driven technologies.

2.1 Sovereignty *de iure* and *de facto*

The misalignment between sovereignty *de iure* and *de facto* is double-faced. On the one hand, what has come to be regarded as nation-state sovereignty *de facto* since the 1648 Peace of Westphalia does not find a coherent reflection *de iure*. Beaulac (2004) notes, indeed, that those institutional, legal, and political arrangements usually associated with the Westphalian order do not find a statutory reflection in the treaties of Münster and Osnabrück which are regarded as the founding documents of that same order. In fact, these documents address issues of religious tolerance, territorial settlements, and legal powers; and yet, they have become *de facto* the pillars for the crystallization of nation-state empires.

On the other hand, sovereignty as established *de iure* has been (and still is) repeatedly redesigned by the realpolitik of global geopolitics. Suffice to think, in this regard, to centuries of colonization, unilateral borders transgression (the latest case is the war in Ukraine) and, more broadly, the enactment of (il)legitimate state power beyond the limits established by law and territory. In this respect, Krasner (1999) arrives to characterize sovereignty as "organized hypocrisy" to the extent that what is declared in official documents gets repeatedly contested, if not subverted, by practice.

2.2 Sovereignty Across Scales

Concerning the second axis, economic trades on a global scale, alongside the reshaping of state's functions, have been identified as factors that diffused the coalescence of territory, authority/power, and community into the nation-state. In recent decades, a new galaxy of authorities and communities have contested the nation-state as the sole legitimate beholder of sovereignty. On the one hand, Ilgen (2003) contends that under the pressure of economic globalization central governments have forfeited part of their power and authority to external actors, leading to forms of multilayered governance, at both supra- and sub-national levels. Current examples of this in Europe are the increasing autonomy allocated to municipalities and the establishment of the EU as a supranational framework. The problem, in this latter respect, is that the EU has designed for itself the role of international regulator without however sufficiently binding power: as Soare (2023) notes, a "perpetual gap" endures between "EU policymaking and national implementation and compliance." In other words, the EU acts as a legislator without full legitimacy, due to a discrepancy between its authority and a well-formed polity upon which to exert power. Irion (2023) adds that, in the context of digital transformation, "the EU is currently producing many new pieces of legislation on digital issues, which may overstretch the capacity of proper implementation by stakeholders and enforcement", thus leaving behind a patchworked policy landscape hard to harmonize.

At the same time, the push towards a diffusion of sovereignty across scales has been favored by new managerialist approaches to the public sector (Pollitt et al. 2007). With the promise of performing more efficiently towards citizens (mostly regarded as consumers), the state apparatus has embraced economic-driven approaches to the delivery of public services, ultimately dislocating functions that were once its own prerogative to sub-national bodies, external organizations, as well as private actors. This links more closely to the third axis of contestation of nation-state sovereignty.

2.3 Transnational Sovereignty

In recent decades, global trade has become an increasingly entangled affairs manifested by the emergence of transnational relations that cut across and remold nation-states' sovereign legitimacy. As Wen (2021) writes, "the development of the global economy has been characterised by the transition towards transnationalized capitalism, within which information and communications technologies have increasingly played a pivotal role in restructuring the global capitalist system." Hence, an accurate understanding of such scenario through the lens of sovereignty, and past the cornerstone of the nation-state, requires undoing conceptual dichotomies such as global-local, as well as public-private.

In this respect, Wasserman (2018) observes that at stake is the remaking of global power relations that "have prompted different ways of thinking about categories such as the 'South,' the 'global,' the 'local'." For instance, the "going out" phase of Chinese companies across the globe – after years of internal state-supported consolidation – has been perceived, especially in the West, as a form of soft power, if not colonisation *stricto sensu*. From this perspective, Chinese companies have been depicted as the *longa manus* of the government in different regions of the globe. However, ground evidence shows a more fine-grained scenario where Chinese companies' trade does not follow one unique party line, but it is rather the result of different and sometimes conflicting visions. Xu (2014) writes that "Chinese firms have created serious challenges for the Chinese government to regulate them at home and overseas"; while Gu and colleagues (2016) reveal the "proliferation of Chinese businesses acting independently or, depending upon ownership, semi-independently of the Chinese state."

To emerge then are federated forms of globalization – contested internally as much as externally – in which the circulation of goods – including data – and subjects, as well as the adoption of regulations, depend on the entrenchment of multifactorial trends building on competing agendas, authorities, powers, and territories. This demands to approach sovereignty by keeping into account the entangled nature of such federated forms of globalisation (Calzati 2020).

2.4 ICT-Based Sovereignty

As seen with transitional sovereignty, ICTs have become pivotal in redesigning sovereignty across public and private actors. ICTs are, at once, cause and effect of the (re)wiring of the globe under commercial pushes. Concretely, the framing of ICTs within a sovereign geopolitical perspective, brings with itself forms of power asymmetry. Studies have shown the "misalignment" between the Internet as a commons infrastructure and the legitimacy of sovereign powers (Mueller 2019). Traditional categories such as "market" and "state", "national" and "international", may no longer be sufficient to account for today's tech-based geopolitics.

For instance, Yu and Goodnight (2020) argue, with specific regard to China, that: "China's so-called Intranet also reveals entanglements with foreign capital, foreign technology, foreign markets, and foreign labor." More specifically, while the US have been heralded as defending a multi-stakeholders "free Internet" and China, on the contrary, as advancing a multilateral "sovereign Internet", the scenario is more complex, with these two competitors often finding agreements behind the scenes especially when it comes

to the very basic principle of surveillance through data. As an example, Gagliardone (2016) writes that in 2012 "representatives at the WTSA were swift in passing a new standard on the 'Requirements for Deep Packet Inspection in Next Generation Networks,' or 'Y.2770.' Discussions happened behind closed doors and no drafts were circulated before a final decision was made, attracting criticism on the lack of transparency." In other words, the agreement on the standardization of deep packet inspection (DPI) did find wide consensus among different actors, even between those (supposedly) heralding opposing views on the Internet's governance.

This means that ICTs have impacted on nation-state sovereignty in multifarious ways, reshaping established power relations, fostering new alliances based on contingent interests, as well as creating preconditions for new asymmetries within and beyond the nation-state.

3 Digital Sovereignty

This brings us to explore the concept of "digital sovereignty". According to Kushwaha and colleagues (2020), "digital sovereignty" is a concept that is mid-way between the broad idea of "technological sovereignty" and the narrow idea of "data sovereignty". In fact, Irion (2023) notes that digital sovereignty remains "conceptually fuzzy and is used to animate a wide spectrum of geopolitical, normative and industrial ambitions"; while Timmers (2023) identifies a stack of at least six layers – "key enabling technologies", "semiconductors", "networks", "data", "cloud services" "apps" – to which digital sovereignty might apply.

Beyond these analytical distinctions, at the heart of the matter is control over data and tech infrastructures (Hummel et al., 2021). Overall, apart from those countries able to chart their own course, the risk of being co-opted by major global tech actors, private or public, is high. At stake, then, is an issue of governance and, most notably, how to account for the distribution of data/tech power across a diversity of actors (Micheli et al. 2020). As scholars (Glasze et al. 2022) point out, technology governance becomes part and parcel of geopolitics when power relations heavily influence how a technology is developed, implemented, controlled, and used.

From this perspective, digital sovereignty can be best regarded as a macro entangled cyber-geopolitical dimension which contests and resists linear (agent-structure) readings on which nation-state sovereignty rests. It is a whole *ecosystemic procedural* dimension that comes into being (see also Sect. 5). For instance, while US corporations tend to dominate Internet services and software, the "ownership" of hardware infrastructures depends on an imbrication of actors. As an example, the transpacific FASTER cable system, connecting the US and several cities in Japan, China, and Korea, was jointly developed by Chinese, American and South Asian private companies. It is evident that such diverse composition questions the epistemological robustness of sovereignty to its state-centric (Westphalian) roots, demanding to account for the enmeshment between technology and geopolitics that digital sovereignty entails.

Luciano Floridi (2017) calls "cut-and-paste" the logic at the basis of digital transformation: "the digital cuts and pastes reality in the sense that it couples, decouples, recouples features of the world". This has deep repercussions on sovereignty as traditionally conceptualized in terms of territory, authority/power, and community.

To begin with, data-driven technologies frame the subject – and turn it into a data subject – regardless of its location: access to a digital infrastructure is all that is needed and sometimes this might be independent from the subject's own will. This implies a schism between the subject's physical and virtual existence, which goes in hand with a redefinition of their rights. The emergence of e-residency programs developed by European countries (e.g., Estonia and Portugal), especially on the wave of the pandemic, is a case in point. E-residents are bestowed with a (location-independent) digital citizenship attached to the country they apply to. For becoming e-residents the monadic fusion of presence and territory is no longer required, insofar as any subject can potentially apply to e-residency programs from/to anywhere in the world. Similarly, the legislation of the country to which the subject has applied – including supra-national frameworks – comes to extend beyond its physical territoriality and it does so by enforcing a digitization of both the (data) subject and physical placedness, which gets virtualized into a non-local space. More broadly, this is a good example of two simultaneous "decouplings", as Floridi (2017) calls them, made possible by the digital transformation: that between location and presence, on the one hand, and that between law and territoriality, on the other. In fact, e-residency programs emerge out of the splitting of these binomials and by leveraging on their recombination, producing an entanglement of its own between the data subject and a set of actors – banks, public authorities, as well as other e-residents – with which the data subject inevitably gets enmeshed.

"Digital sovereignty", then, is a multifaceted concept that cannot be reduced to a linear mapping of the actors involved and their relations. This is so because it is the fundamental attributes of sovereignty – territory, authority/power, community – that the "digital" contributes to remix. It is only when the notion of digital sovereignty is contextualized and approached as an ongoing process needing finetuning that it becomes possible to question who claims power, on whom such power is exerted, for what purposes, and with which consequences.

3.1 Digital Sovereignty of/in the European Union

In February 2020, Ursula von der Leyen (2020) defined digital sovereignty as the capability "to make its own choices, based on its own values, respecting its own rules' in the field of tech." This is a definition of sovereignty that puts the stress on autonomy in the sense of technological self-determination. In fact, already in 2016, the Council of the European Union defined strategic autonomy, which is also applied to digital sovereignty, as the "capacity to act autonomously when and where necessary and with partners wherever possible." These two claims are relevant for two reasons.

Beginning with the latter claim, partnerships are considered as key enablers toward strategic autonomy; and yet, when this understanding is applied in the context of digital sovereignty, partnerships remain more of a wish than a concrete strategy: as Soare (2023) explains unambiguously "the EU does not have a clear idea of what a new approach to tech partnerships should look like [and] it lacks a balanced approach to partnerships." So far, the EU has adopted a rather passive approach in the shaping of its digital sovereignty, largely interpreting "autonomy" as lack of interference from foreign actors. This is mostly done against the disproportionate data grabbing of US-American tech companies, as well as the deployment of infrastructural networks by

Chinese ones. On the one hand, companies such as Microsoft, Google, Amazon have opened datacenters around the continent, to the point that the EU (2019) has warned against the "digital dependency on non-European providers and the lack of a well-performing cloud infrastructure respecting European norms and values", which can de facto be considered as a form of colonization. On the other hand, while initially European countries welcomed Chinese giant Huawei to roll out its 5G network across the continent – partly to reduce dependency on the US, partly due to the unclear national and supra-national legal overlaps (Robles-Carrillo, 2023) – later the project was halted due to possible security risks at national and supra-national levels.

Recent pieces of legislation such as the Digital Service Act (DSA) and the Digital Markets Act (DMA) represent two steps in the direction of a more robust and binding regulation of large private tech platforms and data service providers with the goal to both create a safer digital space in which the fundamental rights of all users are safeguarded, as well as to establish fairer rules towards the boosting of innovation and competitiveness. Other initiatives that aims to promote the EU's autonomy in matter of digital transformation are the "5G toolbox", that is, a comprehensive European framework designed through the coordination of Member States' national policies in matter of adoption and deployment of 5G network; and the European Chips Act aimed to unburden the EU from its dependence on foreign actors as far as the supply of advanced semiconductors is concerned (although this, in turn, questions the impact of such Act on the sovereignty of a third country – Taiwan – which is one of the biggest suppliers of semiconductors globally and a country whose sovereignty is threatened by China).

Leaving aside the difficulty of effectively enforcing all these pieces of legislation in a harmonious way, these initiatives show limitations in two respects. On the one hand, the interpretation of digital sovereignty in terms of lack of interference from foreign actors is not sufficient for achieving a fully formed European digital sovereignty. In this regard, the EU needs to adopt a more proactive stance for instance by promoting bilateral cooperation to defend its own digital assets and develop symmetric power relations, especially with the US and China.

A case in point is the redefinition of the EU open data policy towards non-EU actors, either private or public. China's nation-state approach towards the regulation of its own data landscape is well-known by now; what is less know, however, is that China's initiatives on this matter – recently, the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) – have two complementary effects: to expand the (extraterritorial) outreach of its own legislation, as well as disempower foreign measures negatively impacting its own interests. It is a digital sovereignty that entangles privacy issues with national security; moreover, it is a sovereignty that is centrifugal as far as the outwards impact of China's legislation is concerned, and centripetal as far as the inward securization of its assets – data, infrastructures, services – is concerned.

This is just the latest instantiation of a series of tactical decisions involving the US and China. Already in 2018, the US Cloud Act, which was passed after the adoption by China of its Cybersecurity Law in 2017, represents a policy move that, under the guise of data localization and protection, has an eminently transnational character; to which China responded with its PIPL and DSA (both approved in 2021). The point is that such decisions might also have undesirable commercial repercussions, as it was the case with

the Trump's administration issuing a commercial ban against Huawei in 2019 through a security order. While such ban did impact Huawei's economic performances, some US companies found themselves in an odd position as both Huawei's commercial partners and actors bound to national "duties". This eventually led some US companies to bypass the ban, with FedEx suing the US Commerce Department and Google warning the Trump administration that the ban would constitute a national security risk in its own right. This shows the extent to which "states will increasingly face difficult policy decisions with regard to deciding how best to balance competing sovereign interests" (Kushwaha et al., 2021). In this scenario the EU is reactive rather than proactive, mostly responding to the consolidation of Chinese market dominance and the conjoint effort by the US to renationalize supply chains (Broeders & Kumiska, 2023). Hence, the highlighted lack in the EU of a clear strategy of external cooperation is a clear limitation and might constitute a testbed for designing more symmetric agreements with foreign partners based on shared values and equipollent legislations. These agreements could leverage on the EU's strength as an international regulator and on its digital assets, such as the open data policy which currently risks asymmetrically benefitting a diverse array of actors without sufficient return and safeguards. On this, Voss and Pernot-Leplay (2023) contend that an adequacy determination between China and the EU in matter of data transfer is currently not possible, meaning that a power asymmetry endures.

On the other hand, the EU's policy initiatives tend to privilege the preservation of individual rights, such as privacy – e.g., the DMA aims to "create a safer digital space in which the fundamental rights of all users are protected" – over collective-level rights – such as democratic participation – as well as the pursuing of economic competitiveness – e.g., the DMA aims to "establish to establish a level playing field to foster innovation, growth, and competitiveness" – over the creation of social value. To better understand why such double focus is limiting, von der Leyen's definition of digital sovereignty provided above comes in handy: "to make its own choices, based on its own *values* [italics added]." What are these values? In presenting Europe's digital future in 2020, von der Leyen spoke of the need to enact a digital strategy in which technology works for people, promotes a fair and competitive economy, and foster an inclusive and sustainable society. As we will see below, currently "people" have been reduced to the individual/consumer and central stage has been taken by economic interests and actors, while social and collective-level concerns have fallen into the background.

4 The EU's Strategy and the Gap with Digital Sovereignty

The EU has adopted a human rights-based approach (HRBA) to governing digital transformation (Brown, 2019), which, while being pivotal for preserving individuals' integrity before digital transformation, especially in terms of freedoms and privacy, risks systematically overlooking societal and collective-level values – such as social inclusion, environmental sustainability and digital sovereignty – which cannot be boiled down to individuals and their rights (Smuha, 2021; Taylor et al., 2017; Viljoen, 2021). For instance, Taylor and colleagues (2017) discuss the idea of "group privacy" and the need to redesign current legal frameworks, starting from the acknowledgement that data-driven technologies address and impinge on groups-as-collectives besides and beyond

individuals. Going further, Viljoen (2021) notes that the individualistic vision behind the current EU approach does not account for the relational nature of data and the consequent trade-off effects that data re-use involving two subjects might have on unaware third parties. On this wave, Smuha (2021) suggests taking inspiration from environmental law for tackling potential collective-level effects caused by digital transformation, such as the erosion of the legitimacy and functioning of the rule of law, which can be neither accounted for nor mitigated by the current EU approach to digital transformation Hence, to the extent to which HRBA does constitute the fundamental baseline to citizens' autonomy, it might be insufficient to enact a fully-fledged digital sovereignty, requiring to shape a well-formed polity to be legitimate.

A partial response comes from the Declaration on Digital Rights and Principles of the EU, which defends "a European way for the digital transition, putting people at the center." Notably, what the DDRP does is to pin down six principles – 1) preserve people's rights; 2) support solidarity and inclusion; 3) ensure freedom of choice; 4) foster democratic participation; 5) increase safety, security, and empowerment of individuals; 6) promote sustainability – which equally split between a half (1, 3, 5) focusing on the individual and the other half (2, 4, 6) pertaining to society as a whole. Hence the DDRP does strive to strike a balance between subject-centric and collective-centric dimensions (Calzati, 2022). However, so far, such balance has not been operationalized, constituting a critical point of contention for the enactment of a European digital sovereignty.

Recent documents have laid the ground for the establishment of an EU digital single market (DSM), as the arena where the digital strategy will play out. In this sense, the 2021 Digital Europe Programme speaks of "the importance of building a thriving ecosystem of private actors to generate economic and societal value from data, while preserving high privacy, security, safety and ethical standards." This statement is significant because it clearly places private actors at the centre of the market, endowed with the task of creating economic and societal value. On this point, Taylor (2021) warns against the notorious difficulty of "establishing meaningful accountability for the private sector" which hinders an effective public scrutiny of how tech companies operate, for which purposes, and with which results. The risk is to see the conflation between public value created by the public sector and public value created by businesses "despite the profit interests involved and the different regulatory architectures occupied by firms and government" (Taylor, 2021). While it might occur that private companies do deliver public value, this can hardly occur on a systemic basis, that is, one that keeps into account collective-level tradeoffs beyond a cost-benefit logic.

The subsequent 2022 Digital Europe Programme provides a clearer characterization of the emerging DSM. Here the European Commission speaks of "the deployment of (…) common data spaces, based on (…) a data infrastructure with tailored governance mechanisms that will enable secure and cross-border access to key datasets in the targeted thematic areas." The DSM is a secured technical backbone revolving around private actors and achieving economic-driven and GDPR-compliant data sharing. In a similar vein, in 2019 the GAIA-X project was launched by a nonprofit foundation with the goal to "enable a sovereign decision on data-based business models" and to promote "common models and rules for data monetization", as well as "cross-industry cooperation to create federal, interoperable services" (BMWi, 2020). Most importantly, behind

GAIA-X is a consortium founded by 22 German and French companies supervised by the German Federal Ministry for Economic Affairs and Energy. Albeit being a no-profit foundation, GAIA-X's governance raises concerns about the way in which sovereignty can be actually guaranteed as a collective principle, since it gets dislocated to private actors and placed in the hands of only two countries, without dutiful consultation and orchestration. Literature shows (Monti, 2023) that tech-centered and market-driven policies are relatively weak tools for pursuing digital sovereignty and strategic autonomy, in that these policies can hardly become compasses for political action.

Overall, the individual-centric and economic-driven approach of the EU to digital transformation is at odd with a full-fledged idea of digital sovereignty that maintains a societal and collective outlook by default, able to cut across scales and involving diverse actors. At stake is the need to design an arena that moves away from prioritizing either certain actors – private or state actors – or values – oftentimes economic competitiveness over social inclusiveness or environmental sustainability – to rather enact a systemically balanced ecosystem.

5 An Ecosystemic Proposition

An ecosystem is characterized by homeostasis, that is, the balanced interaction between biotic and non-biotic elements within an environment. This implies that the ecosystem's behavior cannot be studied by isolating either elements or interactions; rather, it must be studied in its entirety. While largely related to the natural world, the notion of ecosystem has also been applied to other settings, such as the digital landscape (van Loenen et al., 2021). To endorse an ecosystemic vision towards the governing of digital transformation means to seek a fair governance in which all actors' interests are accounted for and negotiated. In other words, fairness underscores here the systemic trading off among different interests in view of an overall equilibrium.

This understanding of fairness overcomes both a reductionist and an essentialist definition of the term. Within the first group fall those attempts which seek to provide a mathematical definition of fairness, overlooking its contextual dependency. On the other hand, an essentialist standpoint does account for the context-dependency of fairness, and yet it still considers it as a core quality of a given technology or data process, failing to produce a comprehensive enactment of fairness within a given scenario.

To shift towards an ecosystemic understanding of fairness it is worth looking at how the EU defines this term in the context of the development and implementation of data-driven technologies. Notably, the European Commission disentangles fairness as both a substantive and procedural affair. On this point, Rochel (2021) notes that as a structuring principle of the GDPR "fairness" is "linked to principles such as proportionality and other procedural dimensions of a balancing exercise involving rights and interests." This highlights well the fact that, beyond the matching of certain requirements, fairness is an act of balance based upon the recognition and negotiation among different interests and rights on a flexible and rolling basis. Hence, a governance framework that aims to regulate a data ecosystem fairly identifies roles and rules to represent the data interests of all actors, as well as mechanisms to adjudicate situations where conflicts among actors and/or values might arise. Most importantly, such ecosystem shall be regarded not

much as an arena where different players are connected, but as a process that constantly reshapes its own power relations. It is in this respect that the definition of sovereignty provided in the introduction is particularly fitting in that it regards sovereignty as a process, more than a state of affair. How to enhance such process will occupy the remnant of the paper.

5.1 Data Commoning: Conceptual Tenets for a European Digital Sovereignty

To tackle the situation, it is necessary to rethink democratic participation *through* and *about* digital transformation. Scholars (Zygmuntowski, et al., 2021) have hinted at the promise of designing an EU data governance that is based on the logics of the commons.

Originally, the commons referred to natural resources characterized by non-excludability (i.e., difficulty or impossibility of forbidding access and use of resources to any potential beneficiary) and rivalry (i.e., the use of resources depletes them and reduces further use by others). Ostrom (1990) showed that the self-management of resources by communities can be more effective than market-driven or state-led approaches, provided that principles and roles are designed and abided to. Moving towards the "second wave", by now the commons has been applied to non-natural resources, such as data (Dulong de Rosnay & Stalder, 2020). Today, Data Commons (DC) initiatives aim to counteract and/or repurpose the centralized ownership and use of data – either by tech companies or states – by giving these back to citizens, with the goal to foster sustainable collective data practices (Morozov & Bria, 2018). Overall, DC defines a self-organizational management of data and infrastructures which is non-appropriative by default (knowledge, assets, and outputs are not owned, in the commercial sense of the term, but summoned up and recirculated); collaborative by design (it considers all actors and links within the ecosystem as integral and necessary to the system's flourishing), and collectively sustainable in its goals (indeed, common goods for the community) (Calzati, 2022). This means that the creation of social value – in either tangible or intangible forms – is regarded as desirable on an equal footage with economic value, which is then recirculated within the system.

Bloom and colleagues (2021) suggest how Ostrom's design principles for managing natural resources might be transposed in the context of data initiatives, in terms of access, management and adjudication of resources. However, their standpoint remains anchored to a normative understanding of data as a resource, preventing an effective tackling of data through the lens of the commons (Sanfilippo & Frischmann, 2023).

More useful is to move beyond the conception of the commons as a resource – a thing – to accommodate the idea of "commoning" (de Angelis, 2017) as a sociotechnical process. As de Angelis (2017) notes "commons are not just resources held in common, or commonwealth, but social systems [of] ongoing interactions, phases of decision making and communal labor process." The shift is crucial when applied to data. Indeed, differently from natural resources, data do not pre-exist in nature. Instead, data are a fully artificial (human and/or tech-created) construct that exists in the very moment in which a certain (sociotechnical) process is enacted. Hence, data-as-resource are unique in that they manifest an entangled nature: if one stresses the informational constituency of data, then data are a virtual entity and are potentially distributable globally; if one stresses the technical constituency of data (from collection to storing and use), then data

are material entities whose allocation and circulation can be favored or hindered in many ways. The hybrid nature of data is also responsible for tensions at legal level: someone can claim ownership over data even without control (and vice versa), stressing either the informational (e.g., European doctrine) or technical constituency (e.g., US doctrine) of data. The commoning of data, then, requires a paradigmatic shift in the way to think and manage data: data are always created under certain (sociotechnical) conditions, used for certain purposes, in certain contexts, by certain actors, and with certain results. Decisive, in this regard, is the boundary of the data commoning, and how this boundary negotiates the hybrid nature of data.

In other words, at the core of data commoning is a *certain* idea of polity. A (data) polity is a fractal concept as far as its scale is concerned in that it depends on the interplay among three components: infrastructures, institutions, and people. As long as these components are ideally co-extensive (i.e., they overlap), then authority and territoriality are fully legitimate, as the exercise of power coincides with (and can be scrutinized in) the interest of the whole community. Whenever the co-extensiveness of the three is not guaranteed, as it is often the case – e.g., an international actor comes in play in a given data polity under international market laws – then we have a weakening of legitimacy because of a discrepancy between authority and territoriality. This inevitably implies that the blossoming of a given polity is subjected to ongoing (re)negotiation. Already today, local, national, and supra-national legal frameworks are in place for disentangling individual and collective interests concerning the access and (re)use of (personal) data. This is so because "general interest" is an entangled concept: from an empirical perspective, the concept reflects the diversity of interests of all actors involved in a given situation; from an ethical perspective, it constitutes the synthesis (not necessarily the sum) of all actors' interests. In fact, such synthesis is never given once and for all; rather, it is based on ever-changing discontinuities across the polity and among its actors. Concretely, this demands the design of an iterative process able to reflect upon itself – and its own condition of existence – in a democratic way. The term *communitas* etymologically identifies, not much the sharing of "things", but a *duty to come together* (*cum* + *munus*). This suggests that a data polity moves across a spectrum that fairly negotiates and/or adjudicates between *public* and *private actors*, *collective* and *individual* rights and values, as well as *informational* and *technical* constituencies of data. Most importantly, a data polity comes with rights and responsibilities for contributing to and maintaining the pooling of data; it is as much an issue of *control* as of *care*: in fact, the balancing act between these two poles is what might define an indigenously European digital sovereignty.

For the present discussion the outer horizon of the EU's data polity is European citizens, institutions, and territory. As seen, such characterization shall not be considered monolithically, but as a dimension in constant articulation across scales and contexts. At the same time, the very fact of identifying a European polity turns the issue of digital sovereignty on its head, starting from the premise that there exists such a polity, and it has a continental outreach: as Broeders and Kaminska (2023) argue, "member States must realise that policy coordinated under the EU umbrella is more fruitful economically and geopolitically than national actions." Concerning what lies beyond the EU, digital sovereignty shall be based on systemic fairness as discussed above, notably by drafting symmetric agreements as far as the (societal and economic) value of data is concerned, as

well as based on equipollent legislations as far as the protection of fundamental rights is concerned. This leads to suggests that, based on the categorization of the United Nations Conference on Trade and Development, internally the EU could promote a "light-touch" or fully open data sharing, while externally it should articulate a spectrum going from "strict localization" of data to "conditional soft transfer" based on symmetric agreements. To do so, however, the EU needs to establish for itself a well-formed polity. Three axes are at stake: 1) which actors; 2) which interests; 3) which features of data.

The term "public actors", on the one hand, cuts across scales – from sub-national to EU levels – aligning to the discussion on sovereignty discussed above; on the other hand, it involves both institutional *and* non-institutional actors. In fact, a heterogeneous galaxy of actors does contribute to inform data commoning: NGOs, non-profit organizations, data intermediaries, data stewards, etc. (including free riders). This heterogeneous galaxy is increasingly acknowledged – yet, not operationalized – by the EU (e.g., in the Data Governance Act), for instance identifying data altruism organizations and data cooperatives. The term "private actors" refers to small and medium enterprises, as well as big tech giants and public undertakings. In this respect the modulation of the commoning might depend on several factors, such as size, position in the market, tasks, revenues, etc. On this point, the commoning can builds upon the criteria identified by the DMA and DSA as a compass; however, to reach an effective identification and operationalization of all these actors and factors requires further research.

Concerning individual and collective dimensions, processes of arbitration shall be designed to disentangle and/or adjudicate the most fitting commoning approach whenever conflicts between interests and values arise. Since the Open Data directive, the EU has acknowledged that "means of redress should include the possibility of review of negative decisions." More recently, the Data Act speaks of "settlement bodies" to ensure "alternative ways of resolving domestic and cross-border disputes in connection with making data available." Yet, how to properly design such bodies so that they harmonize legal frameworks across scales and in different contexts remains an open issue.

Concerning the informational and technical constituency of data, governance mechanisms must be designed to either negotiate between the two constituencies of data or disentangle and give priority to either one of the two. The commoning modulation, then, impacts on different levels of access and management (including reuse) of data, depending on the kind of initiative at stake, the type of data, and the actors involved, and their goals. In this sense, the spectrum of commons licenses shall be regarded as a starting point towards all-exhaustive framework able to finetune to different scenarios.

6 Conclusion

The paper firstly discussed how the emergence of a global networked society has shaped digital sovereignty into a cyber-geopolitical entangled affair. Secondly, the paper delved into the EU's understanding of digital sovereignty as technological autonomy and linked this to the EU's digital strategy. On the one hand, such understanding is rather passive compared to competitors and ultimately insufficient to protect and enhance the EU's digital assets (RQ1); on the other hand, by pursuing an individual-based economic-driven digital strategy, the EU hinders the possibility of achieving a fully-fledged digital sovereignty, which maintains a collective horizon by definition (RQ2).

To counteract this, the paper builds upon the idea of data commoning, as a sociotechnical process that can favor the consolidation of a European data polity. Notably, data commoning can accommodate a fair representation, negotiation, and, if needed, adjudication of individual data interests, while keeping a societal and collective outlook. Key, in this regard, are 1) the involvement of both institutional and non-institutional actors on a rolling basis; 2) the definition of data arbitration processes able to cut across scales and contexts and negotiate or adjudicate between individual and collective dimensions; 3) the identification of access rights and managing responsibilities modulated on the premise of pooled data as both informational and technical constituencies. Recent EU's pieces of legislation begin to address points 1 and 2; yet, *how* to systemically design such involvement and arbitration are open questions. Point 3, instead, remains uncharted and requires further investigation.

While laying down the foundation of a European data polity and a possible way to enact it beyond market- or state-oriented approaches, this paper is conceptual in nature. As such, the identified coordinates enabling the envisioned data polity need to be operationalized, ideally in living lab scenarios or through action research, to be validated.

References

Agnew, J.: Mapping political power beyond state boundaries: territory, identity, and movement in world politics. Millennium **28**(3), 499–521 (1999)

Werner, W.G., De Wilde, J.H.: The endurance of sovereignty. Eur. J. Int. Rel. **7**(3), 283–313 (2001)

Loughlin, M.: Ten tenets of sovereignty. In: Walker, N. (ed.) Relocating Sovereignty, pp. 79–110. Routledge, New York (2018)

von der Leyen, U.: A union that strives for more: My agenda for Europe (2020). https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

Grant, M.J., Booth, A.: A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info. Libr. J. **26**(2), 91–108 (2009)

Beaulac, S.: The power of language in the making of international law: the word sovereignty in Bodin and Vattel and the myth of Westphalia. Brill (2004)

Krasner, S.D.: Sovereignty. In: Krasner, S.D. (ed.) Sovereignty. Princeton University Press, Princeton (1999)

Ilgen, T.L. (ed.): Reconfigured Sovereignty: Multi-Layered Governance in the Global Age. Ashgate Pub Limited, Aldershot (2003)

Soare, S.: How to achieve digital sovereignty – a European guide. In: Digital Sovereignty: From Narrative to Policy? pp. 19–24 (2023). https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Irion, K.: The general data protection regulation though the lens of digital sovereignty. In: Digital sovereignty: From narrative to policy? pp. 53–57 (2023). https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Pollitt, C., Van Thiel, S., Homburg, V. (eds.): New Public Management in Europe. Palgrave Macmillan, Basingstoke (2007)

Wen, Y.: The Huawei Model: The Rise of China's Technology Giant. University of Illinois Press, Champaign (2021)

Wasserman, H.: Power, meaning and geopolitics: ethics as an entry point for global communication studies. J. Commun. **68**, 441–451 (2018)

Xu, Y.-C.: Chinese state-owned enterprises in Africa: ambassadors or freebooters? J. Contemp. China **23**(89), 822–840 (2014)

Gu, J., Chuanhong, Z., Vaz, A., Mukwereza, L.: Chinese state capitalism? Rethinking the role of the state and business in Chinese development cooperation in Africa. World Dev. **81**(May), 24–34 (2016)

Calzati, S.: Decolonising 'data colonialism': Propositions for investigating the realpolitik of today's networked ecology. Television & New Media (2020). https://doi.org/10.1177/1527476420957267

Mueller, M.: Sovereignty and cyberspace: Institutions and Internet governance (2019). https://www.intgovforum.org/multilingual/sites/default/files/webform/week13-cyberspacesovereignty.pdf

Yu, H., Goodnight, T.: How to think about cybersovereignty: the case of China. Chin. J. Commun. **13**(1), 8–26 (2020)

Gagliardone, I.: The Politics of Technology in Africa: Communication, Development, and Nation-Building in Ethiopia. Cambridge University Press, Cambridge (2016)

Kushwaha, N., Watson, B, Roguski, P.: Up in the air: Ensuring government data sovereignty in the cloud. In: 2020 12th International Conference on Cyber Conflict, Tallinn (2020)

Timmers, P.: Investment policy for digital sovereignty: From policy to action. In: Digital sovereignty: From narrative to policy?, pp. 25–33 (2023). https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Hummel, P., Braun, M., Tretter, M., Dabrock, P.: Data sovereignty: a review. Big Data Soc. (2020). https://doi.org/10.1177/2053951720982012

Micheli, M., Ponti, M., Craglia, M., Berti Suman, A.: Emerging models of data governance in the age of datafication. Big Data Soc. **7**(2), 1–15 (2020)

Glasze, G., et al.: Contested spatialities of digital sovereignty. Geopolitics, 1–40 (2022)

Floridi, L.: Digital's cleaving power and its consequences. Philos. Technol. **30**, 123–129 (2017)

European Union. (2019). Policy and investment recommendation for trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendationstrustworthy-artificial-intelligence

Robles-Carrillo, M.: European 5G policy: Legal and geopolitical approach. In: Digital sovereignty: From narrative to policy? pp. 58–66 (2023). https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Broeders, D., Kaminska, M.: EU digital sovereignty: when top-down meets bottom-up. In *Digital sovereignty: From narrative to policy?* pp. 9–17 (2023). https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Voss, G., Pernot-Leplay, E.: China data flows and power in the era of Chinese big tech. Northwest. J. Int. Law Bus. (2023). https://doi.org/10.2139/ssrn.4393008

Brown, T.: Human rights in the smart city: regulating emerging technologies in city places. In: Reins, L. (ed.) Regulating New Technologies in Uncertain Times, pp. 47–65. Asser Press (2019)

Smuha, N.A.: Beyond the individual: governing AI's societal harm. Internet Pol. Rev. **10**(3) (2021). https://doi.org/10.14763/2021.3.1574

Taylor, L., Floridi, L., van der Sloot, B.: Introduction: a new perspective on privacy. In: Taylor, L., Floridi, L., van der Sloot, B. (eds.) Group Privacy. PSS, vol. 126, pp. 1–12. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8_1

Viljoen, S.: A relational theory of data governance'. Yale Law J. **131**, 573 (2021)

Calzati, S.: Federated data as a commons: a third way to subject-centric and collective-centric approaches to data epistemology and politics. J. Inf. Commun. Ethics Soc. (2022). https://doi.org/10.1108/JICES-09-2021-0097

Taylor, L.: Public actors without public values: legitimacy, domination and the regulation of the technology sector. Philos. Technol. **34**(4), 897–922 (2021)

BMWi. GAIA-X: The European project kicks off the next phase. Germany Federal Ministry for Economic Affairs and Energy (2020). https://www.bmwk.de/Redaktion/EN/Publikationen/gaia-x-the-european-project-kicks-of-the-next-phase.pdf?__blob=publicationFile&v=13

Monti, G. EU competition law and digital sovereignty. In: Digital sovereignty: From narrative to policy? pp. 46–52. https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Rochel, J.: Ethics in the GDPR: a blueprint for applied legal theory. Int. Data Priv. Law **11**(2), 209–223 (2021)

Zygmuntowski, J.J., Zoboli, L., Nemitz, P.: Embedding European values in data governance: a case for public data commons. Internet Policy Rev. **10**(3), 1–29 (2021)

Ostrom, E.: Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge University Press, Cambridge (1990)

Dulong de Rosnay, M., Stalder, F.: Digital commons. Internet Pol. Rev. **9**(4), 1–22 (2020)

Morozov, E., Bria, F.: Rethinking the smart city: Democratizing urban technology. 5. City Series. Rosa Luxemburg Stiftung, New York (2018). https://rosalux.nyc/rethinking-the-smart-city-democratizing-urban-technology/

Bloom, G., Raymond, A., Tavernier, W., Siddarth, D., Motz, G., Dulong de Rosnay, M.: A practical framework for applying Ostrom's principles to data commons governance. https://foundation.mozilla.org/en/blog/a-practical-framework-for-applying-ostroms-principles-to-data-commons-governance/

Sanfilippo, M., Frischmann, B.: A proposal for principled decision-making: beyond design principles. In: Frischmann, B., Madison, M., Sanfilippo, M. (eds.) Governing Smart Cities as Knowledge Commons, pp. 295–308. Cambridge University Press, Cambridge (2023)

de Angelis, M.: Omnia Sunt Communia: On the Commons and the Transformation to Postcapitalism. Bloomsbury Publishing, London (2017)