INTERNET POLICY REVIEW
Journal on internet regulation

Volume 10 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Safeguarding European values with digital sovereignty: an analysis of statements and policies

Huw Roberts *University of Oxford* huw.roberts95@gmail.com
Josh Cowls *University of Oxford***Federico Casolari** *University of Bologna*
Jessica Morley *University of Oxford*
Mariarosaria Taddeo *University of Oxford; British Library*
Luciano Floridi *University of Oxford*

DOI: https://doi.org/10.14763/2021.3.1575

Published: 30 September 2021
Received: 6 December 2020 **Accepted:** 18 April 2021

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Roberts, H. & Cowls, J. & Casolari, F. & Morley, J. & Taddeo, M. & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Keywords: Digital sovereignty, Data governance, EU values, GDPR, Legitimacy

Abstract: The European Union (EU) has, with increasing frequency, outlined an intention to strengthen its "digital sovereignty" as a basis for safeguarding European values in the digital age. Yet, uncertainty remains as to how the term should be defined, undermining efforts to assess the success of the EU's digital sovereignty agenda. The task of this paper is to reduce this uncertainty by i) analysing how digital sovereignty has been discussed by EU institutional actors and placing this in a wider conceptual framework, ii) mapping specific policy areas and measures that EU institutional actors cite as important for strengthening digital sovereignty, iii) assessing the effectiveness of current policy measures at strengthening digital sovereignty, and iv) proposing policy solutions that go above and beyond current measures and address existing gaps. To do this, we introduce a conceptual understanding of digital sovereignty and then empirically ground this within the specific EU context via an analysis of a corpus of 180 EU webpages that have mentioned the term "digital sovereignty" within the past year. We find that existing policies, in particular those pertaining to data governance, help to achieve some of the EU's specific aims in regard to digital sovereignty, such as conditioning outward data flows, but they are more limited concerning other aims, like advancing the EU's competitiveness and regulating the private sector. This is problematic insofar as it constrains the EU's ability to safeguard and promote its values. The policy solutions we propose represent steps towards the further strengthening of the EU's digital sovereignty and firmer protection of EU values.

This paper is part of **Governing "European values" inside data flows**, a special issue of *Internet Policy Review* guest-edited by Kristina Irion, Mira Burri, Ans Kolk, Stefania Milan.

Introduction

Governments' interest in the "datafied society" (Hintz et al., 2018) as an object of policy and regulation is nothing new, with a long-held recognition that governance protocols (policies, ethics frameworks, and regulations) can be used to reshape the technological infrastructure underpinning society and hence its nature (Floridi, 2018; van Dijck & Poell, 2016). However, the widespread adoption of the term "sovereignty"—a concept loaded with legal and political connotations—to describe authority over the digital is a more recent phenomenon (see Section 2). In particular, this term has gained traction in the context of the European Union (EU), which will be the focus of this paper.

In her 2020 State of the Union Address at the European Parliament, Ursula von der Leyen, President of the European Commission, stated that

> this is [the European Union's] opportunity to make change happen by design, not by disaster or by diktat from others in the world [...] it is about Europe's digital sovereignty on a small and large scale (European Commission, 2020d).

This statement is both a signal of intent and a reflection of a newfound policymak-

ing agenda within the EU. Digital sovereignty is seen as a basis for strengthening the EU's role in an interconnected world, promoting its core interests, and protecting the fundamental values upon which the Union is based, namely, human dignity, freedom, democracy, equality, the rule of law and respect of human rights (art. 2 TEU). As we shall see, von der Leyen's speech was not an isolated case. The term "digital sovereignty" has become increasingly popular among the EU's main institutional actors. However, digital sovereignty lacks a clear definition and is deployed inconsistently across EU policy documents. Even fundamental points are unclear, such as whether digital sovereignty is something that the EU already holds, or whether it is a goal towards which the EU should strive. This lack of conceptual clarity is problematic as it raises questions over the exact aims of the EU and hinders the ability of the EU to garner support behind, and successfully enact, a clear policy agenda.

This paper aims to help dispel the aforementioned conceptual confusion by analysing the concept of digital sovereignty both at a high level and as it is used within the context of the EU. This clarifying analysis has four aims: i) to outline what is understood by digital sovereignty when it is discussed by EU institutional actors and place this within a broader conceptual framework; ii) to map the critical policy measures that the EU has taken, and/or has proposed to take, that are purported to implicitly or explicitly strengthen its digital sovereignty; iii) to assess the extent to which the EU's current policy measures are actually effective in strengthening digital sovereignty, as we conceptualise it; and iv) to propose policy solutions that go above and beyond existing policy measures.

The paper is structured to reflect these aims. In section 1, we highlight the difficulties that arise when seeking to understand what digital sovereignty for the EU might consist of. Section 2 offers a precise conceptual understanding of digital sovereignty, which can be applied to the EU policy-making context. Section 3 analyses a corpus of 180 EU web pages that mentioned the term "digital sovereignty" within the past year to understand the specific policy areas of importance for EU institutional actors and the associated policy measures they have presented as furthering the aim of strengthening digital sovereignty. Section 4 draws the theoretical and empirical analysis together by assessing the extent to which the policy measures identified in section 3 actually strengthen the EU's digital sovereignty, as we conceptualise it in section 2. Section 5 concludes by exploring how the EU can strengthen its digital sovereignty and provide specific recommendations for EU policymakers to this end.

1. Digital sovereignty in the European Union

EU institutional actors have referred to the concept of digital sovereignty for several years (Reding, 2016). However, the term is only more recently gaining high-profile traction among policymakers (Timmers, 2019a). Recently, several of the EU's political institutions have put forward definitions of digital sovereignty and related terms. Ursula von der Leyen, President of the European Commission, has referred to "*tech* sovereignty" as the capacity of Europe "to make its own choices, based on its values, respecting its own rules" (von der Leyen, 2020). A similar understanding of "digital sovereignty" is implicit in the statement of Charles Michel, President of the European Council, who sees digital sovereignty as a means for achieving strategic autonomy which "is about being able to make choices […] this means reducing our dependencies, to better defend our interests and our values" (European Council, 2021). The German Presidency of the Council of the European Union (July-December 2020), in its programmatic manifesto, stressed that EU digital sovereignty involves a strengthening "of [the EU's] broad research base and foster[ing] its growing digital infrastructure and economy, while making sure the continent's core democratic values also apply in the digital age" (Germany's Presidency of the Council of the European Union, 2020). Finally, the European Parliament's Think Tank defines digital sovereignty as "Europe's ability to act independently in the digital world" (Madiega, 2020).

From these statements, it is evident that digital sovereignty is a concept keenly promoted by the EU's political institutions. There is a clear emphasis in these definitions on the EU having the capacity to act independently, in line with its values, with respect to digital technology. However, what constitutes digital sovereignty is not always clearly defined, and the institutions variously speak of "establishing" (European Parliament, 2020), "retaining" (European Commission, 2021a), "defending" (European Commission, 2020e), "bolstering" (Germany's Presidency of the Council of the European Union, 2020), and "achieving" (European Council, 2020) digital sovereignty—all terms that have different policymaking connotations. Moreover, the extent to which it is viable that choices could be made by the EU "independently" is unclear, and the identities of those actors with whom the EU is competing (i.e., those who might also claim digital sovereignty) are frequently unstated.

Considering digital sovereignty with respect to adjacent concepts also evidences this confusion. Some analysts have proposed a substantive difference between "tech" and "digital" sovereignty, whilst for others the terms are synonymous (Burwell & Propp, 2020). Similarly, whilst it is clear that the EU's aim of digital sover-

eignty relates to *strategic autonomy*, the distinction and relationship between the two concepts are often unclear (Timmers, 2019b). Digital sovereignty has been forwarded as a means of furthering strategic autonomy (European Council, 2021) and as the end goal of a policy of strategic autonomy (Eager et al., 2020). However, others consider these terms as interchangeable (European Commission, 2020b).

The lack of clarity and coherence amongst the statements of EU institutions and policymakers as to how digital sovereignty should be understood makes it challenging to assess whether the EU is successfully strengthening its digital sovereignty through policy measures that are said to be performing this function. To evaluate the EU's digital sovereignty agenda systematically, identify its strengths and weaknesses, and monitor its progress, the first, necessary steps are to provide a clear, detailed and robust definition of "digital sovereignty", and to offer a more granular set of criteria as a basis for assessing whether these aims are being met.

There are two approaches for developing a definition of digital sovereignty in the context of the EU's policy agenda. The first is bottom-up and consists of using existing statements by EU policymakers to infer a shared concept that may be specific to the European context. However, as we have shown, statements by EU institutional actors are inconsistent, suggesting that such an exercise may yield a concept of digital sovereignty that is fragmented internally. These statements may also be misaligned externally with the usage of the expression by external actors (e.g., other states), which may only result in further conceptual confusion and the inability to reconcile "European" digital sovereignty with that adopted by other actors. For these reasons, we follow an alternative approach, top-down, which is to propose a more general definition of digital sovereignty that is applicable, among other things, to the EU context and can also be used to assess the EU's policy of digital sovereignty in comparative contexts, for example when the digital sovereignty of the US or China is in question. We start by providing a conceptual analysis of digital sovereignty, in the next section, and then proceed to ground it empirically in the EU context in section 3.

2. Defining digital sovereignty

Whilst the concept of sovereignty has been widely discussed across academic literature (Philpott, 2016), attempts to define digital sovereignty have been more limited. Some scholarship has defined digital sovereignty through analysing the specific EU context (Burwell & Propp, 2020; Leonard & Shapiro, 2019) yet, as mentioned, this approach is inadequate for developing a generalisable concept. Other authors have analysed digital sovereignty conceptually, but these works have focused on

outlining the analytical confusion or discursive practices surrounding the term (Couture & Toupin, 2019; Pohle & Thiel, 2020) rather than putting forward a conceptual understanding that can be effectively operationalised for assessing the EU's digital sovereignty agenda.

In this article, we follow the understanding of digital sovereignty we developed elsewhere as constituting "a form of legitimate, controlling authority" (Cowls et al., forthcoming; Floridi, 2020) over—in the digital context—data, software, standards, services, and other digital infrastructure, amongst other things. Two subsidiary elements of our definition need to be explicated for it to be an analytically useful concept for assessing digital sovereignty in the EU, namely *control* and *legitimacy* as they pertain to authority. We follow Floridi's (2020, p. 371) definition of *control* as

> the ability to influence something (e.g., its occurrence, creation, or destruction) and its dynamics (e.g., its behaviour, development, operations, or interactions), including the ability to check and correct for any deviation from such influence. In this sense, control comes in degrees and above all can be both pooled and transferred.

Concerning *legitimacy*, we follow (Franck et al., 1990, p. 24) in defining this as

> a property of a rule or rule-making institution which itself exerts a pull towards compliance on those addressed normatively because those addressed believe that the rule or institution has come into being and operates in accordance with generally accepted principles of right process.

A notion of public consent underpins the definition of legitimacy we adopt, yet there are several ways in which consent can be understood. Here, we understand consent in terms of the tripartite framework of democratic legitimacy in the European context developed by Schmidt (2013) (itself a modification of Scharpf (1999)), which consists of *input* into the decision-making process that underpins a rule or institution (for instance, democracy), the *throughput* or quality of the process by which decisions are made (including accountability), and the *output* or effectiveness of a rule in achieving the goals of what citizens care about.

The overarching definition of digital sovereignty as "a form of legitimate, controlling authority" is agnostic with respect to where, when and by whom digital sover-

eignty can be held. The definition provides a more flexible view of digital sovereignty insofar as it moves beyond traditional state-centric definitions of sovereignty by acknowledging that authority may also be held by international or supranational bodies, as in the case of the EU. It also provides conceptual space for considering the involvement of private sector companies exerting close control—albeit with questionable, and questioned, legitimacy (Taylor, 2021)—over various aspects of digital life. Furthermore, the definition recognises that multiple agents may simultaneously hold digital sovereignty, indicating the possibility of viewing sovereignty as something which can be shared. We also move away from traditional notions of (digital) sovereignty as necessarily being defined by a fixed physical geography and instead view digital sovereignty as something that can be held across political communities and spatial networks that are not limited to the nation-state (Agnew, 2005). This is in recognition of the fact that not all historical polities have been territorially organised, and that contemporary governance of the digital is, in many areas, not territorially bound. In short, we assume that the concept of "sovereignty" has finally and completely detached itself from that of "sovereign". This helps one understand that it is not the case, for example, that "in a lot of ways Facebook is more like a government than a traditional company", as claimed by Facebook CEO Mark Zuckerberg in 2018 (Farrell et al., 2018), but rather that companies like Facebook and national governments are redefining, through their interactions and equilibria, the sense in which an agent can hold and exercise sovereignty.

One more clarification is necessary before grounding this definition of digital sovereignty in the context of the EU. "Sovereignty" relates to the similar but distinct concept of "governance". In this article, we shall assume that digital sovereignty is the authority to set rules that regulate and *govern* action (relying, we have argued, on legitimacy and control), and hence that the (digital) *governance* process involves the exercise of the capacities afforded, *a priori*, by sovereignty. Sovereignty thus captures the capacity of an actor to act (it is something that is held), while governance concerns the interactions of sovereign actors and the nature of the act itself (it is something that is done).

3. Mapping policies for advancing European digital sovereignty

We now turn to grounding this conception of digital sovereignty empirically in the context of the EU. To do so, we assess a corpus of web pages within the subdomains of the European Commission, European Council, and European Parliament

that explicitly mentioned the term "digital sovereignty" between 10 March 2020 and 10 March 2021 (N=180). The analysis is designed to ascertain the policy areas and associated measures that EU institutional actors consider most relevant to strengthening European digital sovereignty. Identifying these policies serves two purposes. It details the areas of digital sovereignty that are of importance to EU institutional actors. And it provides the foundation for assessing whether the actions taken by the EU, which are claimed to strengthen digital sovereignty, are doing so in reality.

To build this corpus, we used Google's site-specific search function to collect relevant web pages from the European Commission (N = 80), Council (N = 70), and Parliament's (N = 30) official websites [1]. We analysed each result to understand the most common contexts in which digital sovereignty is spoken about by representatives of these three main EU governance institutions (see Annex for a full discussion of methodology). In absolute terms, the data set that resulted from the search query was small enough to allow a manual analysis of each of the 180 articles. However, it contains (to the best of our knowledge) all references to "digital sovereignty" from each website, which reassures us about the completeness of the data set concerning digital sovereignty discourse in the European governance context. This analysis identifies the five key areas and aspects of digital technology that institutional actors most frequently mentioned as important for strengthening digital sovereignty. These are: data governance; constraining platform power; digital infrastructures; emerging technologies; and cybersecurity. In the remainder of this section, we assess each of these in turn. In each case, we identify the stated relevance of each aspect of digital technology to the strengthening of European digital sovereignty, and note the associated policy measures and initiatives, planned or enacted, cited by institutional actors.

3.1. Data governance

In many web pages (N=33), meaningful European control over data is presented as integral to the EU's digital sovereignty. This is often portrayed as a necessity for ensuring that infringements on individual privacy rights are curtailed and maximising the societal and industry benefits that can be gained from personal data. For example, it is claimed that data governance regulation will

1. The specific domains were ec.europa.eu, consilium.europa.eu, europarl.europa.eu. Technically these are third level domains within the second-level europa.eu domain.

> provide for more control for citizens and companies over the data they generate, [which] will **strengthen Europe's digital sovereignty** in the area of data (European Commission, 2020g, p. 1, emphasis ours).

The European Data Strategy was one initiative that is frequently presented in the data set as a means of strengthening European digital sovereignty. It seeks to ensure access to more data for the European economy and to provide citizens and companies with more control over their data, through measures such as encouraging open data, developing data pools and facilitating data sharing (European Commission, 2020g). Specific existing measures cited include the Open Data Directive (n. 2019/1024). This encourages making public sector data more freely available within the EU (Berlin Declaration on Digital Society, 2020), and the Single Digital Gateway Regulation (n. 2018/1724), which was seen to lessen bureaucracy and ease cross-border data flows through its "Only Once Principle", thus "relaunching our economy [and] also … building the EU's digital sovereignty" (European Commission, 2020h).

Earlier data governance measures are also outlined as strengthening EU digital sovereignty. This includes the General Data Protection Regulation (n. 2016/679, GDPR), which strengthened digital sovereignty by "putting individuals in control of their data" and making the EU "a standard-setter in privacy and data protection", as per a recent European Parliament report (Madiega, 2020).

The European Commission's Regulation on the Free Flow of Non-Personal Data (n. 2018/1807, FFDR), which was passed by the European Parliament and the Council in 2018 and which has applied since May 2019, is another policy mentioned as strengthening digital sovereignty in the data set (EURAXESS, 2020). Unlike the GDPR, this regulation is exclusively market-centred: it prohibits national rules requiring non-personal data to be stored or processed in a specific member state, in effect neutering data localisation efforts by individual member states. Before this, at least 22 measures were present that explicitly imposed restrictions on transferring data to another member state, and a further 35 measures that could indirectly cause localisation within a member state (Bauer et al., 2016). [2]

2. As an example, it was the introduction of this policy that forced the UK to introduce a data-offshoring policy for the National Health Service (NHS), with an implied policy of data localisation present prior to this.

3.2 Constraining platform power

A second policy area that is outlined as a priority for strengthening digital sovereignty, albeit less frequently (N=13), is to increase EU control over large, non-European technology companies, in particular "platforms". This is to ensure that relevant measures are effective and enforceable against those companies and thus that they respect EU law and values when operating in Europe. As Internal Market Commissioner, Thierry Breton, outlined in a July 2020 speech, that (digital) sovereignty is (among other things)

> about making sure that anyone who **invests, operates and bids** in Europe respects our rules and values [...] [and about] [...] protecting our companies against predatory and sometimes politically motivated **foreign acquisitions** (European Commission, 2020b, emphasis ours).

The perceived misbehaviour of large American technology companies—and the scarcity of European alternatives—has given momentum to large-scale policy responses by the EU. The release of the Commission's proposals for a Digital Services Act (DSA) and Digital Markets Act (DMA) represent clear moves in this direction. The DSA ascribes "cumulative obligations" to platforms that scale with their size, such that the largest (American) platforms will bear the greatest responsibility. The DMA uses "a set of narrowly defined objective criteria" to define "gatekeepers", who will face obligations for ensuring interoperability and competitiveness in how they operate.

European Council President Charles Michel has referred to both acts—and the Commission's antitrust competition policy—as "unique and undeniable strengths" with respect to European digital sovereignty. Moreover, Michel warned that while the EU is "determined to take up these challenges with the US [...] if necessary, we are ready to lead the way on our own" (European Council, 2021).

3.3 Digital infrastructure

A third policy area that consistently recurs in the data set (N=34) was the need to improve core digital infrastructure, such as data storage capacity. References to strengthening infrastructure in the data set portray doing so as necessary for enabling the EU to act with less reliance on foreign technologies; ensuring that EU companies and data will not be subjected to third-country laws on account of foreign data storage (European Commission, 2020c); improving the competitiveness of EU companies (European Commission, 2020f); and empowering citizens and

business (European Commission, 2021c).

A high-profile example of current EU policy in this area is the Gaia-X project, an initiative by the European Commission, Germany, France, and many others, introduced to resolve the problem of reliance on foreign cloud infrastructures. More recently, in October 2020, member states signed a declaration of cooperation on developing a competitive EU cloud infrastructure (European Commission, 2020f), facilitating data storage within the EU.

Finally, connectivity has been highlighted as a necessary infrastructural requirement for furthering EU digital sovereignty by enabling all EU citizens to have full access to digital opportunities and technologies. In the documents we analysed, the Connecting Europe Facility (CEF)—an EU funding instrument that seeks to promote growth, jobs and competitiveness through targeted infrastructure investment—including digital service infrastructures and broadband networks was often explicitly mentioned.Connectivity across the EU is also seen as necessary for supporting positive economic outcomes in the EU, particularly in light of the disruption caused by Covid-19 (European Commission, 2021c).

3.4. Emerging technologies

Emerging technologies was the policy area most frequently referenced across documents (N=42). They are seen as underpinning "most of the key value chains of the future" (European Commission, 2020c), and thus it is essential to ensure that the development of these emerging technologies is in line with EU values (European Commission, 2020b).

Underlying technologies, such as microelectronics, are an area of particular interest amongst policymakers. Semiconductor technologies are one of seven areas where coordinated plans from member states are encouraged under the NextGenerationEU €750 billion recovery plan, adopted in December 2020, that seeks to stimulate the EU's economy in the wake of Covid-19 (Regulation n. 2020/2094). Following this, the European Initiative on Processors and Semiconductor Technologies was announced, a joint declaration by 20 member states that seeks to lessen the EU's reliance on externally sourced microprocessor technologies through increased investment along the semiconductor value chain. Similarly, the Electronic Components and Systems for European Leadership (ECSEL) initiative seeks to grow Europe's semiconductor capabilities, amongst other things, and has been cited as "proof" of Europe's potential to hold digital sovereignty in the field of microelectronics (European Commission, 2020b).

Another emerging technology which the EU is focusing on is the field of supercomputing, with President von der Leyen promising an investment of €8 billion to develop the next generation of supercomputers (European Commission, 2020d), which are seen as a prerequisite to being competitive in the areas of cloud technologies, AI, and cybersecurity.

Finally, the EU is trying to expand its capacity to develop and regulate artificial intelligence (AI). Von der Leyen has recently stressed that

> Artificial intelligence is a prime example of digital sovereignty. It is an example of our ambition to apply European standards and values to technology deployed in Europe. (European Commission, 2020e)

The EU's AI strategy, outlined in documents such as the Communication on Artificial Intelligence for Europe and the draft Artificial Intelligence Act, seeks to ensure that AI is governed in line with EU values and also promotes competitiveness through improving R&D, skills, and partnering with member states and the private sector.

3.5. Cybersecurity

Cybersecurity is the fifth area where EU policymakers have outlined the necessity of further strengthening digital sovereignty (N=24). Strong cybersecurity is seen as a prerequisite for all the other policy areas already identified, because the protection of data, infrastructures, and business are necessary for a functioning and competitive EU digital economy, and the protection of EU values. This is why cybersecurity is described as "a pillar of the European sovereignty for the future" by the EU Science Hub (2020).

Several existing initiatives have sought to strengthen the EU's digital sovereignty by making it a "standard setter in the field of cybersecurity" (Madiega, 2020), including the Network and Information Security Directive (n. 2016/1148, NIS Directive), which provides legal measures to boost the overall level of cybersecurity in the Union, and the Cybersecurity Act which established an EU-wide cybersecurity certification scheme (EURAXESS, 2020). More recently, the EU's Cybersecurity Strategy for the Digital Decade, published in December 2020, aims to bolster Europe's collective resilience against cyber threats and "describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign [which is] founded on the resilience of all connected services and products" (European

Commission, 2021b). The strategy has three pillars: resilience, technological sovereignty and leadership; building operational capacity to prevent, deter and respond; advancing a global and open cyberspace through increased cooperation.

4. Assessing efforts to strengthen the EU's digital sovereignty

In this section, we assess the extent to which the EU is actually furthering digital sovereignty, as per our definition in section 2, understood in terms of *legitimate control*. We focus our analysis specifically on the five areas that were repeatedly emphasised as important by the EU's political institutions, whilst recognising that the concept of digital sovereignty is not limited to these areas, particularly when other state and non-state actors are considered. For example, establishing a "sovereign internet" through controlling what content can be viewed online is an area of digital sovereignty that is critical to China and Russia (McKune & Ahmed, 2018), but was not mentioned by EU institutional actors in our data set. Here we address these two components of our conceptual definition, *control* and *legitimacy*, in relation to the five areas identified above.

4.1. Control

Let us begin by considering the extent to which the EU has already succeeded in exerting control over the five forms of digital technology it most commonly identifies as impacting its digital sovereignty. First, the EU's data governance approach represents the most developed and instantiated policy measures for strengthening the EU's digital sovereignty. Internally, governance measures assert control over member states, by regulating data flows; this includes the FFDR prohibiting data localisation by member states. Externally, control is asserted by the GDPR and the related case-law of the European Court of Justice (in particular the *Schrems* saga, wherein European judges have imposed restrictions upon international data transfer, invalidating the approach elaborated by the Commission), ensuring that data flows are, as far as possible, subject to the control of the EU and the respect of its values. The implementation of the GDPR is also an example of the so-called "Brussels Effect", which refers to the ability of the EU to regulate the global marketplace unilaterally on account of the size and attractiveness of its market. The territorial extension (Scott, 2014) of the GDPR provides the EU with external control as a regulatory superpower, with incentive mechanisms pushing both the private sector and other governments to follow the EU's regulatory approach (Bradford, 2020). In this sense, market mechanisms provide the EU with a form of control over private sector companies.

Although data governance measures are the most developed area of the digital sovereignty agenda, their efficacy has been questioned. Measures such as the Open Data Directive, FFDR, Single Digital Gateway Regulation improve data efficiencies for governments, companies and individuals respectively, but the extent to which they significantly enhance EU control can be called into question; for example, these measures may slightly improve individual control and EU competitiveness, but it seems unlikely that this approach, by itself, meaningfully challenges the dominance of US technology companies. The efficacy of the GDPR has also been questioned on account of the effectiveness of its enforcement, which heavily relies on the national authorities of members states, leading to possible inconsistencies amongst EU states (European Parliament, 2021; Wagner & Janssen, 2021), difficulties in cross-border cooperation, and due to data protection authorities being generally under-resourced (Massé, 2020). Moreover, the fines given to companies that violate GDPR procedures frequently take a long time to materialise and typically pale in comparison to the revenues of major private sector technology firms.

Turning to the second area we identified in the data set, constraining the power of (non-European) platforms, efforts are mostly still getting underway. As noted, the DSA and DMA have not yet been cast into law, but the intention of the propositions is clear: the creation of a regulatory framework that allows EU authorities to pinpoint and sanction technology companies for a range of controversial practices that fly in the face of EU interests. The successful enactment of these measures would enhance control by allowing targeted measures; however, given that they are in the early stages of the law-making process, it is difficult to determine the likelihood of their success. Caution is merited since it is not uncommon that the legislature waters down the EU legal acts, as was the case with restrictions on the use of remote biometric surveillance in the drafting of the proposed EU AI Act.

However, even if they are easily passed into law, constraining the power of—that is to say, controlling—large platforms is likely to require more than the measures contained in the DMA and DSA. This point is best exemplified by the recent EU and member states' response to Covid-19 digital contact tracing. The development and deployment of accurate, effective, and widely available digital contact tracing apps requires a complex socio-technical system, involving both hardware and software as well as analogue capabilities such as laboratory tests for Covid-19 (Morley et al., 2020). At least 19 EU member states turned to Apple and Google—the two companies that control the software and hence the API of most of the mobile phones on which the apps could run—to provide at least the "exposure notifica-

tion" functionality via API (i.e., Apple and Google provide the functionality to alert individuals when they have been near an individual who has tested positive for Covid-19). Whilst states had control over the risk-scoring algorithm used by individual apps (e.g., deciding the threshold level for risky contact) and what individuals must do if they are notified about a Covid-19 contact, Apple and Google held complete sway over which phone models were compatible with the API (not all were); how the API worked; and crucially for how long they would make the API available. This means that, despite the efforts of EU states to exert greater control over the companies, the latter were able to design the technical framework for the system and thus determine key trade-offs between, for example, preserving privacy and sharing data with public health authorities. Apple and Google also maintained the ability in principle to turn off the contact tracing mechanisms of all those states using the API. In this case, existing regulatory measures did little to protect EU member states from the influence of US technology companies over the digital elements of the pandemic response (Sharon, 2020), and it is unlikely that the provisions contained in the DSA and DMA would have overcome these issues, even had they been in place.

This cautionary tale suggests that any regulatory measures must be accompanied by, among other things, the strengthening of EU infrastructures and industries, the third and fourth areas identified in our analysis. In both of these areas, progress has thus far been relatively limited. Improved cloud infrastructures within Europe would provide more opportunity for EU data to be stored within domestic infrastructures, which would strengthen digital sovereignty by ensuring that data is leveraged for emerging technologies, enhancing EU competitiveness, and governed according to European rules and standards (European Commission, 2020f). However, Gaia-X is not a cloud provider. It is a non-profit organisation conceived as a platform joining up the services of European businesses, which does not seek to compete directly with non-European technology companies. And in fact, Amazon and Google were among the 300 businesses involved in establishing the Gaia-X project (Delcker & Heikkilä, 2020). The Declaration of Cooperation on Cloud by EU member states is a strong signal of intent to improve EU cloud capabilities, yet it is unclear when or how these measures will materialise.

Efforts to support the emerging technologies industry are plagued by similar uncertainty. The intention to strengthen digital sovereignty through increased investment is a step in the right direction for semiconductor technologies, supercomputing and AI technologies. However, investment still pales compared to the EU's economic competitors, specifically the US and China, which has led to calls for further

investment in these areas (Brattberg et al., 2020). For AI in particular, given that the US and China have more permissible environments for innovation (at the expense of ethics), it is questionable as to whether the EU will be able to develop and deploy these technologies in a "competitive" manner (Roberts, Cowls, Hine, et al., 2021).

Finally, in terms of control over cybersecurity—the fifth area—the EU has been exerting increasingly more control in recent years, by focusing on developing Europe-wide cybersecurity standards and certification for companies providing digital technologies and services within the EU. This began with the 2019 Cybersecurity Act and the NIS Directive (Taddeo & Floridi, 2018) and continues with the 2021 Cybersecurity Strategy. Internally, the 2019 Cybersecurity Act helped member states improve their cybersecurity capabilities and established a forum, ENISA, for capabilities building, operational support, and standardisation. Externally, the NIS Directive required international providers to adopt EU standards to access the EU market. The proposed revisions to the NIS Directive and the 2021 Cybersecurity Strategy may successfully enhance this kind of control. However, control in the context of cybersecurity is only one element needed to foster the resilience of systems and the stability of cyberspace; international collaboration and regulation for state behaviour in cyberspace are crucial to this end. This is why it is reassuring that the strategy envisages forms of international collaboration to define international norms and standards that reflect EU core values. Ultimately, how much control the EU will have in the cybersecurity area will depend on how much leadership it will exert in these international, regulatory efforts (Taddeo, 2017).

4.2. Legitimacy

The second fundamental aspect of our definition of digital sovereignty is the normative consideration of legitimacy. We saw above that in the European context, the public consent that the criterion of legitimacy requires can be thought of in three senses, namely *input* (political), *throughput* (procedural) and *output* (performance and efficacy) legitimacy.

In each of these senses, the EU's digital sovereignty agenda can be considered at least somewhat deficient. The EU doubtless has input legitimacy because its functioning is based on representative democracy (art. 10 TEU). However, the EU's input legitimacy is limited because of the lack of direct input that citizens have into its selection or policy agenda, the limitations that flow from the lack of a single shared language and media, and the traditionally "de-politicised", non-partisan nature of decision-making in the EU. The absence of a government that "the people"

can directly vote out as a sign of disapproval is particularly troubling in this regard (Schmidt, 2013). When this is read in line with intense corporate campaigning and lobbying that shapes many of the legislative actions above—with the "Big Five" American technology companies reported to have spent €19m lobbying the EU in 2020 alone (Nicolás, 2021)—the actual input of citizens, and relative impact of this input, can be called into question. This raises critical questions about whether the digital sovereignty agenda has been sufficiently developed "by the people".

Throughput legitimacy is also present within the EU in the sense that relevant documents surrounding process and effectiveness are regularly published (Schmidt & Wood, 2019). However, throughput legitimacy is hamstrung by a perception that EU decision-making is less open and transparent. The largely opaque meetings between the European Commission, Council and Parliament in cases where the Council disagrees on amendments proposed by the Parliament (commonly known as trilogue meetings) are a particularly problematic example. For instance, it was through the trilogue mechanism that a political agreement around the €7.5 billion Digital Europe Programme, which includes funding for supercomputing, cybersecurity, and AI, was reached (European Commission, 2020a). This mechanism is not provided for in EU treaties and may undermine transparency in the legislative process. Significantly, the European Court of Justice has highlighted that "a lack of information and debate … is capable of giving rise to doubts in the minds of citizens, not only as regards the lawfulness of an isolated act, but also as regards the legitimacy of the decision-making process as a whole" (European Court of Justice, 2008, para 59). Having this in mind, the EU judges have stated that the work of the trilogues shall also be available for access insofar as it constitutes a decisive stage in the legislative process (European General Court, 2018). Nonetheless, some argue that transparency over how negotiations are conducted is still deficient due to the limited amount of information being provided (Pennetreau & Laloux, 2021).

This leaves output legitimacy, which is achieved when the digital sovereignty agenda is enacted "for the people", judged in terms of the effectiveness of the measures (Schmidt, 2013). As outlined above in our discussion on control, the EU's policy measures, as well as the relevant case-law of the European Court of Justice, have made substantial progress in some areas, such as ensuring better protection of personal data and that the right to privacy is respected, whilst being more limited in others. More generally, the absence of a clear definition of digital sovereignty amongst EU policymakers and an associated assessment criteria undermines efforts to prove that digital sovereignty has been effectively enacted "for the people".

The potential limitations to the legitimacy of the EU's digital sovereignty agenda

are problematic, especially given that other non-nation-state actors are competing to control critical aspects of digital life (Floridi, 2020; Pasquale, 2017). Consider the actions of large technology companies that we have seen exert considerable *de facto* control over various aspects of digital life, as exemplified in the case of Covid-19 tracing apps. And this control increasingly risks being *seen as* legitimate, which may be sustained by a competing loyalty felt by members of the public to technology companies as *users,* in contrast with affinity with the state as *citizens* (Culpepper & Thelen, 2020). This is problematic, not least because it could shield these companies from stricter governance requirements of the sort we identify here. This, in turn, could ultimately threaten fundamental EU values, with examples of technology companies already undermining workers' rights, including gig economy companies threatening the ability to collectively bargain (Tan et al., 2020; Tassinari & Maccarrone, 2020), and algorithmic bias leading to discriminatory outcomes (Tsamados et al., 2021).

Conclusion and recommendations

Our analysis suggests that the range of policy measures adopted by the EU to strengthen its digital sovereignty is a promising first step, but falls short when assessed against the conception of digital sovereignty that we put forward in section 2. In particular, the EU continues to lack sufficient control over digital technologies to ensure that European values are safeguarded. Moreover, to longstanding questions over the institutional legitimacy of EU policy making have been added questions concerning the increasingly murky role of technology companies as "legitimate" actors, to the extent that the idea of individuals as citizens is under increasing strain in an age when private sector actors command greater loyalty of those same individuals *qua* users. And at a higher level, as our analysis has highlighted, the EU still lacks a clear, coherent vision of digital sovereignty, with different actors from different EU institutions emphasising different domains in which, and mechanisms by which, digital sovereignty should be sought and strengthened. With all this in mind, we propose that the EU prioritise three steps to strengthen Europe's digital sovereignty and safeguard its values. These steps, and the associated recommendations that we propose, are structured around the three core deficiencies our analysis has identified: a lack of clarity and coherence around what is meant by digital sovereignty; limits on the EU's control of digital technology; and threats to its legitimacy in this area.

First, an important step is for the EU to establish a common understanding of and position on digital sovereignty throughout the bloc. By "pooling" sovereignty into

achieving coherent goals regarding the digital throughout the bloc, the EU may be able to maximise its digital sovereignty and hence safeguard more effectively its interests and values. We hope that the definition of digital sovereignty proposed in this article and elsewhere (Floridi, 2020) may provide a good foundation for EU institutional actors to use the term "digital sovereignty" in a more precise manner.

However, even if the EU's position on digital sovereignty were to be made clearer, by itself, this would remain inadequate for effectively controlling large technology companies, most of them not European. Therefore, the EU should strengthen its global reach in that domain, by elaborating legal instruments capable of extending their application beyond the Union's borders; the above-mentioned GDPR approach could represent a benchmark in this respect. At the same time, the EU needs to equip itself with a stronger toolkit to promote and support European technology companies that align with the EU's values and prevent the continued widening of the capability gap between European and non-European companies. A policy of national champions, similar to that adopted in China (Roberts, Cowls, Morley, et al., 2021), has been proposed by some EU institutional actors for boosting competitiveness (Calenda, 2020; Volpicelli, 2020). However, previous efforts to enact similar policies in the EU in the 1980s were disappointing and did little to increase international competition (Strange, 1996). It may thus prove fruitful instead for the EU to assess how member states have maintained a world-leading position in some industries, such as car and aerospace manufacturing, and determine the extent to which related policies can be adopted to foster successful technology companies. The corollary is equally worth stating: the EU should also work to identify the similarities and differences between the technology space and more established sectors, with respect to the effectiveness of the investment capacity, regulatory measures, and policy instruments currently at its disposal. The pre-eminence of Silicon Valley is just the most pronounced of these tech-sector-specific characteristics. However, there are many more, some of which may be more naturally advantageous to EU governance and more reflective of "European values", such as the EU's stated focus on trust and trustworthiness in the context of AI, or potential points of convergence with the EU's globally ambitious green agenda.

Finally, the EU's digital sovereignty agenda is presently undermined by the perceived limitations of the legitimacy of its policy-making processes. Unethical outcomes can arise if the EU is unable to introduce sufficiently strong regulatory measures on account of the perceived "pseudo-"or merely "quasi-legitimacy" held by technology companies through their ubiquity, scope, and their users' loyalty or reliance on them. A clearer digital sovereignty agenda, which is aligned to member

states' understanding of the term, may provide a good foundation as per our first recommendation. However, to improve legitimacy still further, the EU should strive to strengthen transparency within governance and support open democracy initiatives of co-design and co-ownership of policies, stimulating thus social acceptability and public support. [3] One method for doing this is through futures and foresight techniques, which can be used for visioning the type of digital sovereignty towards which EU citizens want to strive. At the same time, a more accurate course of action should be elaborated at the EU level to improve the digital awareness of EU citizens, to allow them to exert a more active role in shaping the relevant measures.

These are only a narrow slice of the wide range of further steps that the EU could take as digital technologies increasingly impact on the lives and livelihoods of EU citizens. Nonetheless, the current efforts identified in our analysis represent an important first step in the EU's efforts to maximise its digital sovereignty. However, as the capacity and complexity of digital technologies continue to grow, it will be increasingly necessary to introduce new and better measures to ensure that the interests of EU citizens are protected, and European values are safeguarded. Arguably, such changes would require a more effective allocation of competences among the Union and its member states, a result which cannot be achieved without amending the existing EU Treaties.

A first occasion for inclusive, high-level reflection on the following steps to be taken towards an agenda for Europe's digital sovereignty is the ongoing Conference on the Future of Europe, where citizens, stakeholders, social partners and academia are empowered to have their say on the EU's future policies and ambitions.

Annex

We used Google's site search function to collect web pages from the European Commission's, Council's, and Parliament's official websites, between 10 March 2020 and 10 March 2021, that explicitly mentioned the term "digital sovereignty". A period of one year was selected because it ensured that the results analysed were reflective of only the most recent discussions of digital sovereignty in the EU context. These results returned 83 web pages for ec.europa.eu, 88 results from europarl.europa.eu, and 67 from consilium.europa.eu, totalling 238 web pages. Once duplicate entries were filtered out, our final corpus was 180 web pages, with 80, 70 and 30 returned from the Commission, Parliament and Council respectively.

3. This need not necessarily be limited to policy-making only with respect to digital technology.

We analysed these webpages to understand the policy areas that were being discussed in relation to furthering digital sovereignty and the associated measures that were being referenced as helping to achieve this. Five key themes emerged from our analysis, which were: data governance, constraining platform power, digital infrastructures, emerging technologies and cybersecurity. The table below outlines the frequency with which each policy area was cited as being of importance with respect to strengthening digital sovereignty.

It is important to acknowledge the potential limitations in our methodology, particularly in relation to the frequency of mentions. Although we filtered duplicate web pages from our results, we did not remove multiple results that referenced the same speeches of prominent EU figures. This led to the policy areas mentioned in some speeches to be repeated multiple times across different web pages, in different contexts. Accordingly, some policy areas received a significant increase in terms of their frequency of mentions due to the recurrence of these speeches across the data set. We did not consider this "echoing" to be problematic. Indeed, it is to be expected that explicit references to digital sovereignty by senior figures will be influential in shaping myriad policy measures pursued by the EU institutions that they represent. Whilst we could have further filtered our data to remove these examples, we believed that this would undermine the perceived relative significance of each policy area.

	EUROPEAN COMMISSION (TOTAL = 80)	EUROPEAN PARLIAMENT (TOTAL = 70)	EUROPEAN COUNCIL (TOTAL = 30)	TOTAL	EXAMPLE POLICY MEASURES
DATA GOVERNANCE	16	15	2	33	European Data Strategy; GDPR; FFDR; SDGR; Open Data Directive; Data Governance Act
CONSTRAINING PLATFORM POWER	2	10	1	13	Digital Services Act; Digital Markets Act
DIGITAL INFRASTRUCTURES	18	9	7	34	Gaia X; Connecting

	EUROPEAN COMMISSION (TOTAL = 80)	EUROPEAN PARLIAMENT (TOTAL = 70)	EUROPEAN COUNCIL (TOTAL = 30)	TOTAL	EXAMPLE POLICY MEASURES
					Europe Facility; Joint Declaration on Cloud
EMERGING TECHNOLOGIES	20	16	6	42	White Paper on AI; European High Performance Computing Joint Undertaking; ECSEL; European Industrial Strategy
CYBERSECURITY	9	10	5	24	Network and Information Security Directive; European Cybersecurity Act; European Cybersecurity Strategy

References

Agnew, J. (2005). Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics. *Annals of the Association of American Geographers*, *95*(2), 437–461. https://doi.org/10.1111/j.1467-8306.2005.00468.x

Bauer, M., Ferracane, M. F., & van der Marel, E. (2016). *Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localization* (No. 30; Global Commission on Internet Governance Paper Series). https://www.cigionline.org/publications/tracing-economic-impact-regulations-free-flow-data-and-data-localization

Berlin Declaration on Digital Society and Value-Based Digital Government at the ministerial meeting during the German Presidency of the Council of the European Union on 8 December 2020. (2020). European Commission. https://ec.europa.eu/isa2/sites/isa/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Brattberg, E., Csernatoni, R., & Rugova, V. (2020). *Europe and AI: Leading, Lagging Behind, or Carving Its Own Way?* [Paper]. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/07/09/europe-and-ai-leading-lagging-behind-or-carving-its-own-way-pub-82236

Burwell, F. G., & Propp, K. (2020). *The European Union and the Search for Digital Sovereignty:Building "Fortress Europe" or Preparing for a New World?* [Issue Brief]. Atlantic Council Future Europe Initiative. 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

Calenda, C. (2020). *Report on a New Industrial Strategy for Europe* [Report]. European Parliament. https://www.europarl.europa.eu/doceo/document/A-9-2020-0197_EN.html

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Culpepper, P. D., & Thelen, K. (2020). Are We All Amazon Primed? Consumers and the Politics of Platform Power. *Comparative Political Studies*, *53*(2), 288–318. https://doi.org/10.1177/0010414019852687

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*, *34*(2), 234–243. https://doi.org/10.1016/j.clsr.2017.09.001

Eager, J., Whittle, M., Smit, J., Cacciaguerra, G., & Lale-Demoz, E. (2020). Opportunities of Artificial Intelligence. Study for the Committee on Industry, Research and Energy, Policy Department for Economic. *Scientific and Quality of Life Policies, European Parliament*, *99*.

EU Science Hub. (2020). *Cybersecurity—Our digital anchor—A European perspective* [Report]. European Commission. https://ec.europa.eu/jrc/en/facts4eufuture/cybersecurity-our-digital-anchor

EURAXESS. (2020). *A Europe fit for the digital age*. https://euraxess.ec.europa.eu/worldwide/south-korea/europe-fit-digital-age

European Commission. (2020a). *Commission welcomes agreement on Digital Europe Programme*. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2406

European Commission. (2020b). *Speech by Commissioner Thierry Breton at Hannover Messe*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1362

European Commission. (2020c). *Europe: The Keys to Sovereignty* (Vol. 11). The Keys To Sovereignty. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en

European Commission. (2020d, September 16). *State of the Union Address by President von der Leyen*. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

European Commission. (2020e). *Statement by the President at 'Internet, a new human right'*. https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

European Commission. (2020f). *Towards a next generation cloud for Europe*. https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

European Commission. (2020g). *Regulation on data governance – Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2103

European Commission. (2020h). *The Once Only Principle System: A breakthrough for the EU's Digital Single Market*. https://ec.europa.eu/info/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-nov-05_en

European Commission. (2021a). *Key Digital Technologies: New partnership to help speed up transition to green and digital Europe*. https://ec.europa.eu/digital-single-market/en/news/key-digital-technologies-new-partnership-help-speed-transition-green-and-digital-europe

European Commission. (2021b). *Cybersecurity Strategy*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Council. (2020). *Remarks by President Charles Michel after the Special European Council meeting on*. https://www.consilium.europa.eu/en/press/press-releases/2020/10/03/remarks-by-president-charles-michel-after-the-special-european-council-meeting-on-2-october-2020/

European Council. (2021, February 3). *Digital sovereignty is central to European strategic autonomy—Speech by President Charles Michel at 'Masters of digital 2021* [Online event.]. https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/

European Parliament. (2020). *EU institutions establish common priorities for 2021 and until next elections*. https://www.europarl.europa.eu/news/en/press-room/20201217IPR94201/eu-institutions-establish-common-priorities-for-2021-and-until-next-elections

Farrell, H., Levi, M., & O'Reilly, T. (2018, April 9). Mark Zuckerberg runs a nation-state, and he's the king. *Vox*. https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133). https://doi.org/10.1098/rsta.2018.0081

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

Franck, T. M. (1990). *The Power of Legitimacy Among Nations*. Oxford University Press.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society*. Polity.

Leonard, M., & Shapiro, J. (2019). *Strategic sovereignty: How Europe can regain the capacity to act* [Policy Brief]. European Council on Foreign Relations. https://ecfr.eu/publication/strategic_sovereignty_how_europe_can_regain_the_capacity_to_act/

Madiega, T. (2020). *Digital sovereignty for Europe* (Briefing PE 651.992; EPRS Ideas Papers). European

Parliamentary Research Service.

Massé, E. (2020). *Two years under the GDPR: An Implementation Progress Report*. Access Now. https://www.accessnow.org/alarm-over-weak-enforcement-of-gdpr-on-two-year-anniversary/

McKune, S., & Ahmed, S. (2018). The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda. *International Journal of Communication*, *12*, 3835–3855. https://ijoc.org/index.php/ijoc/article/view/8540

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature*, *582*(7810), 29–31. https://doi.org/10.1038/d41586-020-01578-0

Nicolás, E. S. (2021). *Big Five' tech giants spent €19m lobbying EU in 2020*. https://euobserver.com/science/151072

Pasquale, F. (2017, June 12). From territorial to functional sovereignty: The case of amazon [Blog post]. *Law and Political Order Blog*. https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/

Pennetreau, D., & Laloux, T. (2021). Talkin' 'bout a Negotiation: (Un)Transparent Rapporteurs' Speeches in the European Parliament. *Politics and Governance*, *9*(1), 248–260. https://doi.org/10.17645/pag.v9i1.3823

Philpott, D. (2016). Sovereignty. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2016/entries/sovereignty/

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Reding, V. (2016). *Digital Sovereignty: Europe at a Crossroads*. EIB Institute. https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf

Roberts, H., Cowls, J., Hine, E., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). *Governing Artificial Intelligence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes* (SSRN Scholarly Paper).

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. *AI & SOCIETY*, *36*(1), 59–77. https://doi.org/10.1007/s00146-020-00992-2

Scharpf, F. (1999). *Governing in Europe: Effective and Democratic?* Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198295457.001.0001

Schmidt, V. A. (2013). Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput'. *Political Studies*, *61*(1), 2–22. https://doi.org/10.1111/j.1467-9248.2012.00962.x

Schmidt, V. A., & Wood, M. (2019). Conceptualizing throughput legitimacy: Procedural mechanisms of accountability, transparency, inclusiveness and openness in EU governance. *Public Administration*, *97*(4), 727–740. https://doi.org/10.1111/padm.12615

Sharon, T. (2020). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-020-09547-x

Strange, S. (1996). *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge

University Press. https://doi.org/10.1017/CBO9780511559143

Taddeo, M. (2017). Deterrence by Norms to Stop Interstate Cyber Attacks. *Minds and Machines*, *27*(3), 387–392. https://doi.org/10.1007/s11023-017-9446-1

Taddeo, M., & Floridi, L. (2018). Regulate artificial intelligence to avert cyber arms race. *Nature*, *556*(7701), 296–298. https://doi.org/10.1038/d41586-018-04602-6

Tan, Z. M., Aggarwal, N., Cowls, J., Morley, J., Taddeo, M., & Floridi, L. (2020). *The Ethical Debate about the Gig Economy: A Review and Critical Analysis*. https://doi.org/10.2139/ssrn.3669216

Tassinari, A., & Maccarrone, V. (2020). Riders on the Storm: Workplace Solidarity among Gig Economy Couriers in Italy and the UK. *Work, Employment and Society*, *34*(1), 35–54. https://doi.org/10.1177/0950017019862954

Taylor, L. (2021). Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector. *Philosophy & Technology*. https://doi.org/10.1007/s13347-020-00441-4

Timmers, P. (2019a). Challenged by 'Digital Sovereignty'. *Journal of Internet Law*, *23*(6).

Timmers, P. (2019b). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2021). The ethics of algorithms: Key problems and solutions. *AI & SOCIETY*. https://doi.org/10.1007/s00146-021-01154-8

van Dijck, J., & Poell, T. (2016). *Understanding the promises and premises of online health platforms*. Big Data & Society. https://doi.org/10.1177/2053951716654173

Volpicelli, G. (2020, February 20). Who will really benefit from the EU's big data plan? *Wired UK*. https://www.wired.co.uk/article/eu-tech-data-industrial

von der Leyen, U. (2020). *Shaping Europe's digital future*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260

Published by

in cooperation with