

Digital sovereignty

A new key concept of digital policy
in Germany and Europe

Julia Pohle



Digital sovereignty

**A new key concept of digital policy
in Germany and Europe**

Julia Pohle

Imprint

Published by:

Konrad-Adenauer-Stiftung e. V. 2020, Berlin

Contacts at the Konrad-Adenauer-Stiftung:

Jason Chumtong

Policy Advisor for Artificial Intelligence

jason.chumtong@kas.de

Sebastian Weise

Policy Advisor for Innovation

sebastian.weise@kas.de

Cover Image:© shutterstock/Morphart Creation; iStock by Getty images/
simonkr; unsplash/Markus Spiske

Design and typesetting: yellow too, Pasiiek Horntrich GbR

This publication was published with financial support
of the Federal Republic of Germany.



This publication is published under a Creative Commons License:
CC BY-SA 4.0 international (<https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

ISBN 978-3-95721-841-4

At a glance:

- › Striving to strengthen digital sovereignty, self-determination and strategic autonomy has become a cornerstone of German and European digital policy. Within Germany and Europe there are diverging notions of digital sovereignty.
- › However, a common or at least consistent understanding of what is meant by this or what its associated requirements are, has yet to emerge. In particular – but not exclusively – in the political sphere, we can see that this concept is tied to various interpretations and associations.
- › The many different meanings attached to the concept of digital sovereignty in Germany and Europe could be broken down and categorized in three levels, within which a strengthening of digital sovereignty is strived for. These are the state, the economy and the individual. There are always considerable conflicts of interest between these dimensions of digital sovereignty. Between these dimensions, conflicts of political objectives arise that cannot be resolved.
- › In order to leverage the potential inherent in the concept of digital sovereignty for a more strategic and holistic digital policy, not only conceptual work and political will is required. It is also necessary to reflect on what a liberal and democratic understanding of sovereignty actually stands for in the digital age.

Content

Introduction	5
1. The origin and meaning of the concept of digital sovereignty	6
2. Demands for digital sovereignty in Germany and Europe	9
2.1 The debate on digital sovereignty in Germany	10
2.2 The digital sovereignty discourse at European level	11
3. Digital sovereignty in Germany: dimensions and areas of implementation	14
3.1. State dimension	14
3.2. Economic dimension	15
3.3. Individual dimension	16
Conclusion: Democratic sovereignty in a digital Europe	19
Bibliography	21
The Author	26

Introduction

In July 2020, in its programme for Germany's EU Presidency, the German government announced its intention to "establish digital sovereignty as a leitmotiv of European digital policy" (Bundesregierung, 2020, p. 8). This prominent example is only one of many that show the extent to which the idea of "digital sovereignty" has developed into a key concept in debates about digitalisation in the last few years. Particularly since the public outrage following former CIA agent Edward Snowden's leaking of details of extensive surveillance by the US secret service and its allies in the summer of 2013, the demand for digital – or technological – sovereignty can be regularly found in strategy and position statements of German government policy and appears just as frequently in commentaries by economic and societal actors. Also at the European level and in other European states, there are consistent calls for greater self-determination and strategic autonomy with regard to technology and the digital economy. These calls serve as shorthand for the aspiration to reduce the dependency on digital infrastructures and services from foreign providers, notably the US. The global circumstances of the coronavirus pandemic and its accompanying changes have added weight to the calls for more independence and decision-making capacity in the digital sphere.

However, a common or at least consistent understanding of what is meant by this or what its associated requirements are, has yet to emerge. In particular – but not exclusively – in the political sphere, we can see that this concept is tied to various interpretations and associations. Furthermore, nearly all actors, regardless of their economic, political or technical affiliation, use it almost exclusively in a prescriptive-normative way (Couture & Toupin, 2019; Misterek, 2017). On the one hand, the actors' demands convey a desire for states, private enterprise organisations and individuals to be able to manage the challenges of increasingly important digital connectivity. On the other hand, many of the statements mainly formulate abstract objectives for German or European digital, economic and industrial policy, which are not specifically named or systematically implemented.

This research paper breaks down and categorises the many different meanings attached to the concept of digital sovereignty in Germany and Europe.¹ To that end, it analyses the origin of the concept and its discursive function at German and European level. It also suggests a systematisation of related policy measures based on three dimensions. Finally, it makes some observations for a democratic understanding of digital sovereignty.

1 An earlier version of this text focussing solely on the debate in Germany was originally published in Klenk T., Nullmeier F., Wewer G. (editors) "Handbuch Digitalisierung in Staat und Verwaltung" (Handbook of digitalisation in state and administration). Springer VS, Wiesbaden. 2020. The author would like to thank Leo Thüer for his content-related and editorial support and Thorsten Thiel for his conceptual input.

1

The origin and meaning of the concept of digital sovereignty

Regardless of its use in the digital context, the term sovereignty refers to the ability to act in a self-determined manner, free from foreign domination.² The traditional understanding of sovereignty was strongly influenced by 16th century political theorist Jean Bodin and his idea that the ultimate decision-making power and the sole right to use force in a state ought to lie with the ruler – the sovereign. In the 18th century, the Enlightenment philosopher Jean-Jacques Rousseau heralded a radical shift in the understanding of the concept, from ruler’s sovereignty to people’s sovereignty. Along with the development of modern democracies, the idea prevailed that a people in its entirety carried the highest state power but could entrust it to a ruler or an elected government to exercise it.

The term’s legal interpretation is also formative for a modern understanding of sovereignty, where it represents a legal entity’s capacity for self-determination. This is characterised by self-reliance and independence and thus represents a contrast to external determination while still differing from complete autarchy and/or isolation. In constitutional and international law, sovereignty refers to the independence of a state from other states (external sovereignty) and its self-determined domestic state organisation (internal sovereignty). The idea of sovereignty is also closely linked to that of the territorially demarcated nation state: a state is sovereign if, compared to other states, it can act largely independently in political, economic and societal terms.

In modern democracies, the term sovereignty is inextricably linked to the principle of rule of law. A democratic state’s sovereignty involves securing the ability of its citizens to self-determination with their inalienable rights. It thus serves the purpose of enabling all persons to be respected in their own personal rights and to act on their own authority. Guaranteeing the general conditions for this is seen as the state’s responsibility, not least in view of the many challenges that the digital transformation poses for all areas of society.

The specification “digital” in the concept of “digital sovereignty” therefore refers less to the adjective which, in contrast to “analogue”, describes the characterisation due to use of computers or the internet. Instead, it refers to the macrosocial transformation process of digitalisation, characterised not only by the overarching use of computer technology, but primarily by two related trends: the spread of digital connectivity and the marked increase of digital data collections and cross-border data flows.

In light of these trends, a concept of sovereignty that is linked too closely to the idea of a nation state with a demarcated territory is seen by many as outdated (Friedrichsen & Bisa, 2016, p. 1; Lambach, 2019). Intensified by universal globalisation, increased digital connectivity with its continuously growing cross-border data flows is creating stronger dependencies and ties between states and rendering them even less able than ever to act in a self-determined and independent manner. Such increased digital connectivity is therefore viewed as a challenge to the economic, political and legal self-determination of nation states and their citizens.

Perceiving digital transformation as a threat to exercising sovereignty is mainly fuelled by three aspects: Firstly, the powerful and central position of a handful of companies is placing the material and immaterial power over vital infrastructures of social life in the hands of private enterprise (Kapczynski, 2020). The commercial orientation of the internet began in e-commerce and in the business providing access to the internet. Over time, however, this orientation has been increasingly characterised by the business in advertising and data and the strategic leveraging of network effects. The result of this trend is today often called platform capitalism or surveillance capitalism (Pasquale, 2016; Zuboff, 2019). In this new form of capitalism, central actors – the intermediaries (such as Google, Facebook, etc.) – not only have enormous resources but also exert a powerful influence over the creation and regulation of markets, the provision and structuring of audiences as well as on access to the basic goods of everyday life (Staab, 2019). In this way, they are increasingly intervening in the roles of states and undermining their ability to self-regulate. This development makes it difficult to clearly differentiate between state and non-state areas of activity such as in law enforcement. In many countries, particularly in Europe, this is leading to fierce criticism and the demand for stronger regulation of intermediaries.

A second aspect is the paradoxical response of a number of democratic states – notably Germany – to the Snowden revelations in 2013. These revealed the almost uncontrolled exercise of hegemonic power and virtually endless possibilities for data collection, analysis and control by US and other Western secret services and technology companies. But the findings about their behaviour as quasi-sovereign, non-territorial entities surprisingly did not lead to an attempt to politically and legally counteract such an agglomeration of power (Steiger et al., 2017) while the public was outraged, intelligence and security cooperation between the United States and Germany has been marked by continuity instead of disruption. The rather insubstantial debate over a so-called “No-Spy-Agreement” between the United States and Germany is just one telling example of the disconnect between public discourse and governmental action, as is the recent intelligence service regulation. This article considers why and where the “Snowden effect” has been lost on different discursive levels. We analyze and compare parliamentary and governmental discourses in the two years after the Snowden revelations by using the Sociology of Knowledge Approach to Discourse (SKAD). Instead, they triggered demands in many countries for digital spaces that are largely uncoupled from global data flows and enable stronger national control of communication, data and law enforcement.³ Since the Snowden revelations, calls for national (or regional) sovereignty in the digital domain have therefore not only become considerably louder but are also often justified by the risks of foreign surveillance and manipulation.

Another aspect is the search for an alternative normative framework with which European and German digital policy can and should align itself. In the past few decades, the internet and its services, the types of usage as well as digitalisation in general have been mainly characterised by a US, strongly capitalist, individualistic and techno-positivistic view, which was able to spread worldwide via the technologies themselves and through dominant business models (Bellamy Foster & McChesney, 2011; Clark, 2016). In the last decade, this perspective has increasingly been challenged by China’s digital policy with its centralised and authoritarian focus, which, due to the ever stronger market position of Chinese IT companies and the state-sponsored Belt and Road Initiative (BRI), also continues to grow (Jiang, 2010;

Kohlenberg & Godehardt, 2018). Within the framework of this international system conflict, there are regular calls for an independent digital regulatory approach in Europe and Germany, oriented towards European standards and values and thus providing an alternative to the US and Chinese models.

Against the backdrop of these varied developments, the current demands for digital and/or technological sovereignty in Germany and Europe can be seen as a desire for more freedom to act and organise, so the actors can help shape the process of digital transformation according to their own values and act autonomously in the digital sphere. In the same way as the traditional understanding of sovereignty, the capacity for self-determination in the digital space represents the middle ground between external determination and autarchy, while distancing itself from both. Such an idea of digital sovereignty can refer not only to the state but also to individual citizens or companies. Therefore, the concept of digital sovereignty, as it is currently used in Germany and other European countries, also encompasses the ability of individuals as well as state or commercial institutions to make autonomous use of digital technologies and to independently and securely exercise their roles in times of digitalisation.

2 The word sovereignty comes from the Latin *superanus* (chief, principal) and entered the German and English language via the French word *souveraineté*.

3 Eva-Maria Kirschsieper, Director of Public Policy at Facebook Germany, assures that her company strives to maintain the balance between law enforcement and users' privacy (Kirschsieper, 2016, p. 243).

2

Demands for digital sovereignty in Germany and Europe

Naturally, the return to the importance of the state and its exercising of sovereignty in the digital space started well before 2013.⁴ The general perception in the first decades of the internet's spread was characterised by very strong scepticism and a rejection of state interference. It was emblematically expressed in the "Declaration of the Independence of Cyberspace" by the internet activist John Perry Barlow (Barlow, 1996), but also left clear traces in academic and political discourse (Johnson & Post, 1996; Wu, 1997, see also Chenou, 2014). Since the early 2000s, however, we can see that states not only show a growing political interest in stronger control of digital developments, but also intervene increasingly in a regulatory capacity. In politics, society and academia, the need for state regulation and enforcement in the digital space has been increasingly accepted. This implied the rejection of the idea that the internet and its evolution had taken place without any state influence (Eriksson & Giacomello, 2009; Lessig, 1999; Mazzucato, 2013).

At the same time, it seemed that national borders had not lost their importance in the digital space, as was often predicted in the early days. While it is not always possible to localise the internet's application layer, the digital infrastructure is nevertheless strongly anchored in physical reality. Its users can always be associated with a specific geographic location. Both authoritarian and democratic states use this circumstance to monitor, control and censor the exchange of communication and data, for example, to suppress defamatory statements and dissident opinions, to protect intellectual property rights or to counter disinformation and illegal activities. However, the relevant measures always apply only to the users and providers of digital services and technologies in the respective country. Therefore, we can increasingly differentiate between various sub-spaces in the digital space, in which different legal standards apply and are enforced with varying levels of success, for example, those for the protection of personal rights or freedom of speech (Mistereck, 2017, p. 14ff).

But the calls for digital sovereignty go beyond confirming and enforcing interventions by the state in the digital sphere. Originally, mainly autocratic countries such as China and Russia invoked the term sovereignty to justify their foreign and domestic digital policies (Arsène, 2020; Budnitsky & Jia, 2018; Creemers, 2020). But in the last few years, the concept of digital sovereignty has developed into a powerful political discourse in Europe and other democratic countries such as India or Brazil, too, aimed at re-establishing the nation state – including its citizens and economy – as a relevant category in global and national processes for coordinating and regulating the digital sphere (Abraham, 2013; Belli, 2019; Pohle & Thiel, 2019). A fundamental difference to the digital sovereignty efforts of illiberal states is the fact that maintaining or strengthening digital sovereignty is shown in democratic countries to be an effective means of preserving liberal values and ideas of order in the course of the digital transformation. In contrast, the sovereignty concept in autocratic states serves to secure state power and make use of new ways for maintaining autocratic structures to suppress potentially democratising effects of the digital sphere (Claessen, 2020; Creemers, 2020;

Jiang, 2010; Maréchal, 2017). Apart from such content-related differences, the digital sovereignty debate in illiberal and democratic states mainly differs in that it is considerably less consolidated in democracies and accompanied by uncertainties as to how the varied demands and announcements can or should be implemented in political, economic and technological practices.

2.1 The debate on digital sovereignty in Germany

Among its European neighbours, Germany is undoubtedly the country that is currently most active in shaping and driving the debate on digital sovereignty – both at national and increasingly at European level. In contrast to other democratic countries such as France or India, the autonomy debate in Germany did not take shape until 2013. Three tendencies characterise the current trend of the German debate: an increasing differentiation and diffusion of the concept into broader areas, the associated renunciation of a traditional understanding of sovereignty, and finally, a strongly normative justification logic that thus far has only been hesitantly communicated outside Europe.

Not least as a reaction to the tangible sense of the digital supremacy of foreign secret services and technology companies, the initial focus of politicians and societal actors after 2013 was on issues of securing digital infrastructures and the associated independence from US (and, of late, also Chinese) providers. Additionally, economic and industrial policy demands and measures assumed a central position early on. On the one hand, this is about protecting the IT infrastructure and data of German companies and, on the other hand, about fostering the competitiveness and independence of Germany as an economic and technology location. While these aspects continue to dominate the debate in Germany, the arguments have indeed diffused and spread into many more areas. In the process, users of digital technology in particular moved into the foreground of the perception of many actors, together with the demand to promote “consumer sovereignty” or “citizen sovereignty” by strengthening digital literacy and user rights and through measures for transparency and reduced complexity.

In the many, often very disparate demands of governmental bodies, academia, business and civil society, we can now see a departure from the traditional understanding of the term sovereignty. Instead of stressing the state's independence and authority in the digital sphere, digital sovereignty is presented as the prerequisite for contributing to the process of digital transformation and for the ability to act autonomously in the digital sphere without having to abandon the use of technologies and providers located abroad. This not only emphasises the democratic state's sovereignty but indeed that of its citizens as individual users and consumers. As a result, the focus is not just on collective sovereignty as the state's ability to act and organise, but also on individual sovereignty, understood as the individual's autonomy and self-determined ability to act in a connected world. Modelled on the recognised concept of “informational self-determination”, it is also often referred to as “digital self-determination” (Mertz et al., 2016).

Although collective and individual digital sovereignty are in many respects mutually dependent, the realisation of digital self-determination of individuals has other prerequisites and consequences than those of a state or an economy. Creating and maintaining it also poses other challenges for politics, administration and society. Not only the definitions of digital sovereignty, but also comprehending what needs to be done to maintain it, therefore vary immensely in the German discourse. However, what unites nearly all the discourse threads is a mainly prescriptive-normative application of the digital sovereignty concept. On the one hand, it is associated with recommended actions, but used much less frequently to designate existing or previously implemented measures or even an actual status. On the other hand, the demands are very strongly substantiated by pointing to a return to European values, goals and universal basic rights – above all, the right to privacy but also to human dignity, to freedom, rule of law, equal treatment, diversity, tolerance and appreciation (Fokusgruppe “Digitale Souveränität in einer vernetzten Gesellschaft”, 2018, p. 2). Using this rhetoric, German actors also try to present a clear alternative concept of a digital economy whose values and business models are strongly dominated by overpowering US and Chinese intermediaries.

What is striking on the one hand is the fact that German politics engages very intensively with the concept of digital sovereignty domestically, with the result that it appears in the latest coalition agreement and in the range of topics of numerous ministries and various political commentaries. The German EU Presidency programme of July 2020, in which the strengthening of Europe’s digital sovereignty receives special attention as one of the core issues, can therefore be interpreted as the strategic and very prominent continuation at European level of what began as a domestic debate (Bundesregierung, 2020). On the other hand, the German government has so far shown much more restraint in using the concept in multi-lateral forums at global or non-European level. The worry is too great that using the term would play into the hands of authoritarian countries and, in the eyes of the Western world, would position the German government on the side of the supposed opponents of a free, open internet – the very ones it wants to distance itself from through the idea of digital sovereignty. Against this background, the German chancellor Angela Merkel outlined her idea of digital sovereignty in her opening speech at the 14th Internet Governance Forum (IGF), organised by the United Nations and hosted by Germany in 2019. Merkel clearly differentiated her understanding of the concept from isolation, protectionism and state censorship, and emphasised instead that it can also be an “expression of sovereignty to advocate a joint, free, open and secure global internet” (Bundeskanzlerin Merkel, 2019).

2.2 The digital sovereignty discourse at European level

Even before Germany’s current EU Presidency, the impact of the German discourse regarding digital sovereignty was already apparent at European level and is, apart from the French influence, one of the most formative factors. But unlike the German debate, the use of the sovereignty concept with reference to the digital sphere by the European Commission and other EU actors is not only less established but also more narrowly focused. On the whole, three tendencies can be identified with a view to the European discourse: a preference for alternative terminology along with

a closely related focus on digital infrastructures and the competitiveness of the EU; very strong continuity with existing work programmes; and finally a justification logic which, while also normatively charged, is less focussed on the individual than the German discourse.

At EU level, the term digital sovereignty has almost never been used or only in exceptional cases. The EU Commission, in particular, prefers to use the terms “strategic autonomy” and “technological sovereignty” (Bauer & Erixon, 2020).⁵ The concept of strategic autonomy, introduced in 2016 in the EU’s “Global Strategy for Foreign and Security Policy”, has a strong overlap with the current use of the sovereignty concept while placing much greater emphasis on the strategic importance of multi-lateral relationships and partnerships (European External Action Service, 2016, p. 3; Lippert et al., 2019). Strategic autonomy can thus also be seen as a means of strengthening (state and economic) sovereignty (Timmers, 2019, p. 2). The difference to the concept of digital sovereignty is mainly that the idea of strategic autonomy was characterised in the context of a military/security policy discourse and is therefore accompanied by a far more specific focus on security and defence issues (ibid., p. 3). While strategic autonomy does not explicitly focus on technology or digital connectivity and technology but at the most covers issues relating to cyber security, the term “digital strategic autonomy” has also been heard on occasion. The associated demands are often limited to strengthening the security of digital infrastructures and technologies. However, they also go beyond that by mentioning support for a competitive European technology sector and the development of strategic alliances (Eurosmart, 2019; Timmers, 2019).⁶

The term technological sovereignty (or “tech sovereignty”), which is frequently encountered at EU level, is even closer to the predominant understanding of digital sovereignty in the German discourse. In order to attain technological sovereignty, the EU Commission focuses primarily on competition (e. g., in the field of artificial Intelligence), building infrastructure (e. g., by supporting broadband and 5G networks) and developing key economic and technological skills to reduce dependencies (European Commission, 2020a). The European discourse thus appears to be considerably more narrowly defined than the German one, which places a lot more attention on the individual sovereignty of users. While the EU Commission is also calling for stronger digital literacy and a conscious approach to digital technologies, it hopes to achieve this goal merely as a secondary result of a new role of the EU as a global leader in the digital economy (European Commission, 2020b; von der Leyen, 2020). Strengthening the European position relative to economic competitors such as the US or China currently appears to be prioritised over the EU’s own aspiration to educate its citizens in dealing with digital technologies.

What is striking is the fact that the various economic and security policy goals set out at EU level in recent years in the context of technological sovereignty do not represent any substantive innovations compared to the European Commission’s previous digital policy programmes. Consequently, the three pillars of the “Digital Single Market Strategy” (European Commission, 2015, p. 3) already largely correspond to the task areas and objectives for strengthening technological sovereignty, as mentioned in the new Commission’s digital strategy of 2019. The difference relates specifically to applying and adapting previous measures to current technology developments, especially in the field of artificial intelligence and quantum computing (European Commission,

2020b). In the heated discussions at EU level about the digital tax envisaged by France or about granting 5G licences to the Chinese technology provider Huawei, existing digital policy goals and topics were also often only supplemented by new terminology and developments as a means of linking them to current discourse, in this case, the digital sovereignty debate.

Linking the idea of the EU's competitive technological sovereignty to the defence of European values can be seen as one of the most important results of this discussion and of the economic and geopolitical tensions of the last few years. Ursula von der Leyen, the Commission's new president, defined technological sovereignty as "the capability that Europe must have to make its own choices, based on its own values, respecting its own rules" (von der Leyen, 2020, p. 3). Concentrating on European values can be understood here, as in the German discourse, as a differentiation from economic and industrial policies pursued by the US and China but also as an emphasis on European social and consumer policies (Steiner et al., 2020, p. 4). Axel Voss, a German MEP from the European People's Party, defined a "European way of digitization, which contrasts with the US-American or Chinese approach and is human-centered, value-oriented and based on the concept of the social market economy" (Voss, 2020, p. 1). Despite this normative justification of sovereignty efforts, the European discourse differs from that of Germany in that it focuses far less on the ability of individual citizen to act and make decisions. At European level, individual self-determination in the digital sphere is not (or only very rarely) formulated as a goal in itself that must be worked towards using targeted measures. Rather, it is portrayed as one of the many positive consequences of technological sovereignty that is based on security, competitiveness and innovation.

4 See Pohle & Thiel (2019) for a detailed discussion of the tensions between sovereignty and digital connectivity and their historic development.

5 The term "digital resilience" also arises in isolated cases in this context. To date, however, it has been used only in a very limited way, for example, with regard to companies and states dealing with security risks or to individual users dealing with digital technologies.

6 Most recently, some authors have attempted to establish the concept of digital strategic autonomy also in the German discourse where it has not been or only rarely been applied thus far. In doing so, the authors are clearly setting themselves apart from a concept of digital sovereignty that also includes companies' and individuals' ability to act. They define strategic autonomy in the digital space as "the capabilities of the state to implement its own political, social and economic priorities without being restricted to an undesired degree by dependencies in digitalisation" (Kar & Thapa, 2020, p. 10).

3

Digital sovereignty in Germany: dimensions and areas of implementation

In the current German debate, at least three different dimensions can be identified – the governmental, economic and individual dimension of digital sovereignty. These dimensions can be allocated to specific areas of implementation and policy areas, but also overlap.⁷

3.1. State dimension

The discussion about the digital and technological sovereignty of the German state and of European states is clearly dominated by security and domestic policy tasks. Under the influence of the public reaction to the Snowden leaks, the coalition agreement between CDU, CSU and SPD in December 2013 was the first one to announce various measures aimed at regaining technological sovereignty. They were to consist of fostering trusted IT products and using national IT security technologies. At the same time, the German government at the time promised further technical options for counter-surveillance, such as expanding the capacities for cyber defence of the Federal Office for Information Security (BSI), which is tasked with pre-emptively fostering information and cyber-security across the state, economy and society.

Security policy measures also include the drafting by the Federal Ministry of the Interior (BMI) of legislation for increasing the security of information technology systems. The IT security act (IT-Sicherheitsgesetz) came into force in 2015 and obligates the operators of critical infrastructures such as energy, water, healthcare or telecommunications to increase the IT security of their networks. The establishment of the Central Office for Information Technology in the Security Sector (Zentrale Stelle für Informationstechnik im Sicherheitsbereich, ZITiS) in April 2017, also by the BMI, should also be mentioned. Also closely related to the debate about digital sovereignty is the agency for innovation in cyber security (Agentur für Innovation in der Cybersicherheit) which is due to be established shortly, and is tasked with developing ambitious cyber security technologies with strategic benefits for domestic and foreign security and making them ready to meet the needs of the German army. As a side effect, the agency, which is allocated to the Federal Ministry of Defence (BMVg) and the BMI, is also tasked with strengthening national and European technologies and expert systems, thus ensuring Germany's and Europe's technological sovereignty (Boeck, 2018).

Of late, the public administration's digital sovereignty has been in the foreground as a new focus topic (BMI, 2019). This is mainly about reducing German administration's dependencies on foreign software providers by promoting open interfaces and standards in the public administration's IT (IT-Planungsrat & IT-Rat, 2020, p. 1–2). The range of tasks planned by the German government and the EU Commission for securing their digital sovereignty is therefore largely of a technical nature and refers to the protection of digital infrastructure and the strengthening of data protection in the digital

sphere. An example would be more comprehensive encryption of communication flows and mandatory retention of data on European soil. However, the range of these actions also encompasses non-technical tasks, such as updated terms and conditions for public entities purchasing software or the efficient implementation of the European General Data Protection Regulation (GDPR).

3.2. Economic dimension

In many cases, policy measures for securing the sovereignty of the state and its core infrastructures have an economic dimension, because they intend to protect data and technical infrastructure of German companies or aim to foster the competitiveness and technical independence of Germany as an economic and technology location. In addition, a multitude of dedicated economic and industrial policy actions are discussed in terms of securing digital sovereignty in the economic area, aimed at counteracting the tangible sense of dependency on foreign digital companies and Germany's and Europe's poor innovative ability. In 2015, a focus group of the national IT summit (IT-Gipfel) elaborated "Guidelines of Digital Sovereignty" and specifically called for the development of key competencies and technologies in the field of software and hardware development, cyber security, big data, smart data as well as the cloud service. The group also recommended that, by fostering the digital internal market in Europe, Germany was to create a competitive economic and innovative space that was dominated by an understanding of technology as an opportunity, not as a risks (BMW, 2015, S. 55). Various trade associations formulated similar recommended actions, for example the BITKOM (Federal Association for Information Technology, Telecommunications and New Media), Germany's largest trade association of the information and telecommunications industry, which also advocates streamlining the process of founding IT start-ups (BITKOM, 2015, p. 16).

Many of the recommendations mentioned were adopted in 2016 by the Federal Ministry for Economic Affairs and Energy (BMW) in its "Digital Strategy 2025". According to this strategy, the BMW's spectrum of digital policy tasks is to sustainably and effectively strengthen data security and "data sovereignty" in Germany, where the latter means that data should be protected against misuse and that users and consumers should be able to make sovereign decisions about the use of their data (BMW, 2016, p. 33). Apart from the security policy measures for which the BMI is responsible, BMW is working to achieve the envisaged data sovereignty through measures such as a cross-border application of electronic identification, a qualified electronic signature, an electronic trust seal for companies and government agencies and data protection certification for cloud services (BMW, 2016, p. 35). The BMW also established a monitoring process for digital sovereignty, as part of which an expert report on competencies for Digital Sovereignty was published in 2017. Along with the state as a regulating instance, this report also addresses other actors and recommends, among other things, providing employees and customers with the tools to help them make better informed decisions. This could be achieved, for example, by the envisaged seal of quality for digital products or customer-friendly privacy statements and general terms and conditions with standardised text elements and symbols (BMW, 2017, p. 72).

Since 2018, the focus has also been on measures and demands relating to new key technologies and new digital business models. Consequently, the national Digital Summit (“Digital-Gipfel”) hosted by the BMWi in 2019 established a focus group entitled “Digital Sovereignty in a Networked Economy” consisting of representatives of ministries, academia and business, whose reports thus far have dealt with issues of sovereignty with reference to artificial intelligence and platform-based ecosystems. The numerous requirements expressed therein do not differ fundamentally from earlier suggestions but clearly emphasise the importance of a connected economy (e. g., through interoperability and co-operation models) and of transparent algorithms (Fokusgruppe “Digitale Souveränität in einer vernetzten Wirtschaft”, 2019). These principles are also prioritised in the idea of a European cloud service Gaia-X announced at the same Digital Summit in 2019 and jointly driven by Germany and France. The project aims to use a common standard to create an open, secure and trusted European platform for small to medium-sized cloud providers. The aim is to offer an alternative to the world’s largest providers, Amazon, Google and Microsoft, which upholds European values and data protection standards on the one hand and to promote a European data innovation ecosystem and the competitiveness of individual providers on the other (BMWi, 2020).

3.3. Individual dimension

A strikingly large number of recommendations aimed at strengthening the digital sovereignty of Germany’s economy and industry contains components affecting the digital literacy and user rights of German consumers. The industry association BITKOM summarises these aspects under the term “user sovereignty”: While “provider sovereignty” relates to the autonomous manufacturing of digital technologies, services and platforms, “user sovereignty” enables companies and customers to make autonomous use of them (BITKOM, 2015, p. 13). Therefore, the economic and individual dimensions of digital sovereignty reveal strong overlaps not only in thematic terms. The measures for securing the digital sovereignty of individuals, which relate largely to education and consumer policies, often include an economic policy component that recognises individual users as consumers of digital products and as workers in an increasingly digitalised economy.

That individuals’ sovereignty in their role as consumers of digital services needed to be protected was, however, emphasised long before the political debate about digital sovereignty started in Europe. The “Charter for Consumer Sovereignty in the Digital World” published by the Federal Ministry for Food, Agriculture and Consumer Protection (BMELV) in 2007 contained core principles for a consumer-friendly design of digital products and services and emphasised the importance of IT security as a guarantee for the right to informational self-determination (BMELV, 2007). Today, protecting digital consumer sovereignty focuses on citizens’ opportunities and skills to make use of digital technologies responsibly and autonomously. In 2017, the Advisory Council for Consumer Issues (“Sachverständigenrat für Verbraucherfragen, SVRV”), an advisory body of the Federal Ministry of Justice and Consumer Protection, defined digital sovereignty as the consumers’ ability to act and as his/her freedom of choice to assume different roles in the digital world, i. e., as market participants, consumer-citizens of a society as well as ‘prosumers’ in social networks (SVRV, 2017, p. 3). In

addition to recommendations for developing digital literacy through media education, the expert report issues proposals for regulating digital services, e. g., condensing general terms and conditions and making it mandatory to disclose algorithms to enable their compliance with applicable laws to be checked.

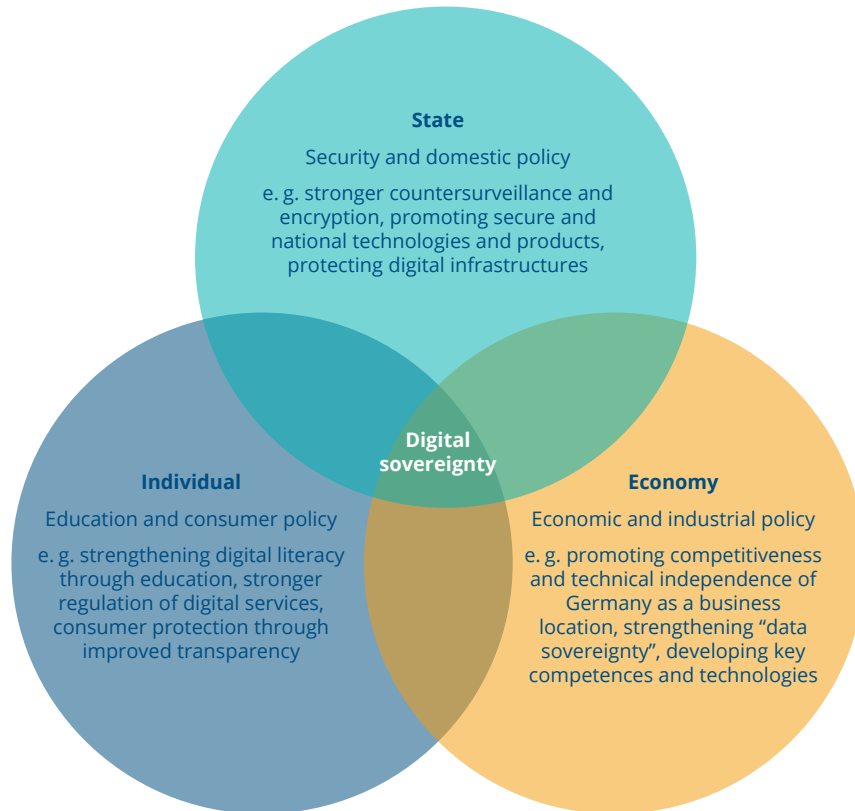
One core aspect that also assumes great importance in the general debate concerning all dimensions of digital sovereignty is consumer-oriented data protection. This is to be ensured, among other things, by user-friendly and data-efficient default settings for communications and other digital services, based on the principles of Privacy by Design and Privacy by Default. Instead of leaving the responsibility for protecting and securing one's own data to the individual consumer, these kinds of provisions and basic settings of technical services will strengthen their trust in digital offerings (SVRV, 2017, p. 9). At the same time, it is frequently emphasised, particularly in terms of data protection, that great importance should be accorded to the individual's self-determination and self-responsibility. Any user of digital offerings should be able to decide for themselves, depending on the context, how much personal data they wish to disclose (IT-Planungsrat, 2013, p. 45).

In addition to the overlap of the individual and economic dimensions of digital sovereignty, we can also see a conflation with the state dimension. The discussion of security and domestic policy aspects reveals the self-determined approach to digital services and technologies to be a prerequisite for mature, digitally sovereign citizens and employees. The IT Planning Council – Germany's political steering body for IT coordination ("IT-Planungsrat") – defines digital sovereignty as the abilities and possibilities of individuals and institutions to independently, autonomously and securely exercise their roles in the digital world (IT-Planungsrat & IT-Rat, 2020, p. 1). Likewise, in a 2019 call for tender, the Federal Ministry of Education and Research (BMBF) seeks to increase digital sovereignty through teaching of competencies and critical reflection skills in dealing with digital technologies and in analysing security aspects (BMBF, 2019b).

Not only consumer protection, but also the development of digital literacy in all stages of life is therefore seen as the basis for sovereign action in the digital world. In spring 2019, a great deal of effort went into an agreement on the digitization in schools ("DigitalPakt Schule"), which aims at improving the provision of digital technology in schools and the relevant qualifications of teaching staff. By responsibly managing digital learning infrastructures, it also seeks to foster the media and digital competence of students and, in the long term, their opportunities in the labour market. Based on the demands of the IT Planning Council in 2013, these competencies should also be developed among politicians in order to enable them to evaluate and shape digitalisation policies in a sovereign manner and in step with the times (IT-Planungsrat, 2013, p. 10). What is remarkable about the demands of the IT Planning Council is the fact that it sees the users as the ones with the responsibility and duty to acquire the necessary expertise for digital sovereignty, thus placing far greater emphasis on individual responsibility. As a result, the Council clearly deviates from the consumer protection perspective as well as from positions that highlight the economic and state dimensions of digital sovereignty. Instead, proponents of these dimensions attribute individual digital sovereignty much more to external conditions, consisting of technical, economic and educational offerings and regulatory frame-

works. After all, only if the necessary prerequisites can be created at a collective level, each individual can decide autonomously how he or she wishes to deal with the challenges and opportunities of digitalisation.

Figure 1: Dimensions of digital sovereignty and fields of implementation



Dr Julia Pohle/privat

7 A rather comprehensive list of planned and implemented measures for strengthening Germany's digital sovereignty can be found in the German government's official reply (publication no. 19/11445) to a parliamentary question by MPs Manuel Höferlin, Frank Sitta, Grigorios Aggelidis and other FDP MPs (Bundestag publication no. 19/10952) from July 2019. It emphasises, among other things, that numerous non-listed measures are largely borne by the private sector and merely backed by the state. Therefore, the state cannot be seen as the sole driver or defender of digital sovereignty.

Conclusion: Democratic sovereignty in a digital Europe

Analysing the debate in Germany and at EU level shows that a strong economic and security policy perspective on digital and/or technological sovereignty is establishing itself in democratic states. Most of the recommended actions aim at securing a future-proof digital infrastructure and the competitiveness of the German and European economy. In terms of the digital sovereignty of individuals, particularly prominent in Germany, the dominant perspectives are those of consumer protection, which perceive citizens primarily as consumers of digital services and technologies. This view, however, harbours the risk of narrowing the strive for digital sovereignty into a purely economic and security strategy. Thus, the different dimensions of digital sovereignty often seem to compete against each other. In particular, the frequent emphasis by political actors of European values, user rights and the social market economy often appears in this contest more as a justification of the preferred security and economic policies than as a consistent distinction from radical market logics or authoritarian value systems.⁸ This not only expresses the reality that, despite the frequent use of the term digital sovereignty across various political camps, it is almost impossible to find a value-based and content-related draft of the concept. It is also clear that a focus on the economy and security in times of digitalisation cannot satisfy the complex issues regarding the capacity for action and for self-determination of every individual and of the state as the entirety of all citizens.

In a democracy, sovereignty falls to the people. Therefore, for a democratic position on individual and collective self-determination in the digital sphere, it cannot be enough to merely emphasise not only the state's, but also the citizens' decision-making authority, or to repeatedly announced the plan to tame the power of private actors through democratically legitimised regulation and control. Rather than continuing to insist on strengthening and enforcing digital sovereignty in a globally connected economy, actors in Germany and Europe should set themselves the task of developing an understanding of digital self-determination which focuses even more clearly on democratic values and a democratic understanding of state than it has been the case thus far. Such an understanding, which prioritises the capacity for democratic self-determination of all citizens, must be clearly demarcated in content and normative terms from the sovereignty discourse of authoritarian states, which instead emphasises sovereign exercising of power by the state. This calls for serious consideration of the question as to what democratic control and accountabilities of sovereign powers should look like in the digital sphere. The digital transformation of all societal areas leads to shifts in the existing balances of power between state, economy and citizens. It is therefore all the more urgent to develop models and mechanisms of how to democratically legitimise and control sovereign exercise of power. This is the only way to gain a European unique selling proposition from the possibilities and potentials of digital connectivity. The current debates about digital sovereignty might therefore provide the opportunity to advance the ideas of European Enlightenment into the digital era and to once again resolve conflicts about the citizens' self-inflicted immaturity – in the interests of digital self-determination.

-
- 8 Therefore, public strategies for digital sovereignty have so far scarcely focused on citizens' rights. The Free and Open Source Software initiative and the Digital Rights movement, strongly represented in Europe and Germany, and the values they represent, such as openness, decentralisation and participation, would be a good fit here.

Bibliography

A Abraham, S. (2013). The Fight for Digital Sovereignty. *Economic & Political Weekly*, XLVIII (42). <https://cis-india.org/a2k/blogs/epw-vol-xlvi-42-october-19-2013-sunil-abraham-the-fight-for-digital-sovereignty>

Arsène, S. (in press). China, Information Technology and Global Freedom of Expression. A story of sovereignty and global capitalism. In L. Bollinger & A. Callamard (eds.), *Regardless of Frontiers. Global Freedom of Expression in a Troubled World*. Columbia University Press.

B Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. <https://www.eff.org/cyberspace-independence>

Bauer, M., & Erixon, F. (2020). Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. *ECIPE European Centre for International Political Economy*, 02, 42.

Bellamy Foster, J., & McChesney, R. W. (2011, March). The Internet's Unholy Marriage to Capitalism. *Monthly Review*, 62(10).

Belli, L. (2019). BRICS countries to build digital sovereignty. *CyberBRICS*. <https://cyberbrics.info/brics-countries-to-build-digital-sovereignty/>

BITKOM. (2015). Digitale Souveränität Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa [Digital sovereignty: Positions and initial recommendations for actions for Germany and Europe]. <https://www.bitkom.org/Presse/Anhaenge-an-Pls/2015/05-Mai/BITKOM-Position-Digitale-Souveraenitaet1.pdf>

BMBF. (2019b). Mensch-Technik-Interaktion für digitale Souveränität. Bundesministerium für Bildung und Forschung [Human-technology-interaction for digital sovereignty. Federal Ministry of Education and Research]. <https://www.technik-zum-menschen-bringen.de/foerderung/bekanntmachungen/digisou>

BMELV. (2007). Charta Verbrauchersouveränität in der digitalen Welt [Charter for Consumer Sovereignty in the Digital World]. Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz [Federal Ministry for Food, Agriculture and Consumer Protection]. https://www.vzbv.de/sites/default/files/mediapics/charta_digitale_welt_1532007.pdf.

BMI. (2019). BMI intensiviert Aktivitäten zur Stärkung der digitalen Souveränität in der öffentlichen Verwaltung. Bundesministerium des Innern, für Bau und Heimat [Federal Ministry of the Interior, for Building and Homeland intensifies activities to strengthen digital sovereignty in public administration]. <http://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html?nn=9390260>

- BMWi. (2015).** Leitplanken Digitaler Souveränität [Guidelines of Digital Sovereignty]. Nationaler IT-Gipfel. https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1
- BMWi. (2016).** Digitale Strategie 2025. Bundesministerium für Wirtschaft und Energie [Digital Strategy 2025. Federal Ministry for Economic Affairs and Energy].
- BMWi. (2017).** Kompetenzen für eine Digitale Souveränität. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie [Competencies for Digital Sovereignty. A study by order of the Federal Ministry for Economic Affairs and Energy]. <https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.html>
- BMWi. (2020).** GAIA-X: A Federated Data Infrastructure for Europe. Bundesministerium für Wirtschaft und Energie. <https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html>
- Boeck, M. (2018).** Technologiesouveränität erlangen – die neue Cyberagentur. Bundesministerium der Verteidigung [Gaining technological sovereignty – the new cyber agency. Federal Ministry of Defence]. <https://www.bmvg.de/de/aktuelles/technologiesouveraenitaet-erlangen-die-neue-cyberagentur-27996>
- Budnitsky, S., & Jia, L. (2018).** Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613.
- Bundeskanzlerin Merkel, A. (2019, November 26).** Rede zur Eröffnung des 14. Internet Governance Forums [Opening Speech at the 14th Internet Governance Forum]. <https://www.bundeskanzlerin.de/bkin-de/aktuelles/rede-von-bundeskanzlerin-angela-merkel-zur-eroeffnung-des-14-internet-governance-forums-26-november-2019-in-berlin-1698264>
- Bundesregierung. (2020).** Together for Europe’s recovery. Programme for Germany’s Presidency of the Council of the EU 2020. <https://www.eu2020.de/eu2020-en/programm>
- C Chenou, J.-M. (2014).** From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. *Globalizations*, 11(2), 205–223.
- Couture, S., & Toupin, S. (2019).** What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(10), 18.
- Claessen, E. (2020).** Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: The case of Russia and the EU. *Journal of Cyber Policy*, 5(1), 140–157.

Clark, D. D. (2016). The Contingent Internet. *Daedalus*, 145(1), 9–17.

Creemers, R. (2020). China's Conception of Cyber Sovereignty. In D. Broeders & B. van den Berg (eds.), *Governing Cyberspace: Behavior, Power and Diplomacy* (p. 107–145). Rowman & Littlefield.

- E** Eriksson, J., & Giacomello, G. (2009). Who Controls the Internet? Beyond the Obstnacy or Obsolescence of the State. *International Studies Review*, 11(1), 205–230.

European Commission. (2015). A Digital Single Market Strategy for Europe. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192>

European Commission. (2020a). Shaping Europe's Digital Future. https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Commission. (2020b). White Paper on Artificial Intelligence: A European approach to excellence and trust https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European External Action Service. (2016). Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. <https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy>

Eurosmart. (2019). 10-Point Manifesto for European Digital Strategic Autonomy. Eurosmart – The Voice of the Digital Security Industry. <https://www.eurosmart.com/towards-european-digital-strategic-autonomy-digital-sovereignty/>

- F** Fokusgruppe "Digitale Souveränität in einer vernetzten Gesellschaft" [Focus group "Digital sovereignty in a networked society"]. (2018). *Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen* [Digital sovereignty and artificial intelligence – prerequisites, responsibilities and recommendations for action].

Fokusgruppe "Digitale Souveränität in einer vernetzten Wirtschaft" [Focus Group "Digital Sovereignty in a Networked Economy"]. (2019). *Digitale Souveränität im Kontext plattformbasierter Ökosysteme* [Digital sovereignty in the context of platform-based ecosystems].

Friedrichsen, M., & Bisa, P. (2016). Einführung – Analyse der digitalen Souveränität auf fünf Ebenen [Introduction – Analysis of digital sovereignty on five levels]. In M. Friedrichsen & P.-J. Bisa (eds.), *Digitale Souveränität* (p. 1–6). Springer Fachmedien.


- I** IT-Planungsrat. (2013). *Zukunftspfade Digitales Deutschland 2020* [Future Paths Digital Germany 2020]. TNS Infratest.

- IT-Planungsrat & IT-Rat. (2020).** Eckpunktepapier Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung [Key Issues Paper Strengthening the Digital Sovereignty of Public Administration] (Nr. 2020/19).
- J Jiang, M. (2010).** Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, 30(3), 71–89.
- Johnson, D. R., & Post, D. G. (1996).** Law and Borders – The Rise of Law in Cyberspace. *Stanford Law Review*, 48, 1367–1402.
- K Kar, R. M., & Thapa, B. E. P. (2020).** Digitale Souveränität als Strategische Autonomie. Umgang mit Abhängigkeiten im digitalen Staat [Digital sovereignty as strategic autonomy. Dealing with dependencies in the digital state]. Kompetenzzentrum Öffentliche IT; Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.
- Kapczynski, A. (2020).** The Law of Informational Capitalism. *Yale Law Journal*, 129(5), 1460–1515.
- Kirschsieper, E.-M. (2016).** Datensouveränität im digitalen Zeitalter [Data sovereignty in the digital age]. In M. Friedrichsen & P.-J. Bisa (eds.), *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft [Data sovereignty: Trust in the network society]* (p. 237–246). Springer VS.
- Kohlenberg, P. J., & Godehardt, N. (2018).** Chinas globale Konnektivitätspolitik [China's global connectivity policy]. *German Institute for International and Security Affairs. SWP-Aktuell*, 18 (März 2018).
- L Lambach, D. (2020).** The Territorialization of Cyberspace. *International Studies Review*, 22(3), 482–506.
- Lessig, L. (1999).** *Code: and other Laws of Cyberspace*. Basic Books.
- Lippert, B., von Ondarza, N., & Perthes, V. (2019).** European Strategic Autonomy. Actors, Issues, Conflicts of Interests (SWP Research Paper 2019/RP 04). German Institute for International and Security Affairs.
- M Maréchal, N. (2017).** Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. *Media and Communication*, 5(1), 29–41.
- Mazzucato, M. (2013).** *The entrepreneurial state: Debunking public vs. private sector myths*. Anthem Press.
- Mertz, M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C., & Woopen, C. (2016).** *Digitale Selbstbestimmung [Digital self-determination]*. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres).

- Misterek, F. (2017).** Digitale Souveränität: Technikutopien und Gestaltungsansprüche demokratischer Politik [Digital sovereignty: technological utopias and requirements of democratic politics] (MPIfG Discussion Paper Nr. 17/11; p. 40). Max-Planck-Institut für Gesellschaftsforschung.
- P Pasquale, F. (2016).** Two Narratives of Platform Capitalism. *Yale Law & Policy Review*, 35(1), 309–319.
- Pohle, J., & Thiel, T. (2019).** Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses [Digital networking and sovereignty: genealogy of a contested relationship]. In I. Borucki & W. Schünemann (eds.), *Internet und Staat. Perspektiven auf eine komplizierte Beziehung* (Bd. 127, p. 35–56). Nomos.
- S Staab, P. (2019).** Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit [Digital capitalism: market and domination in the economy of scarcity]. Suhrkamp Verlag.
- Steiger, S., Schünemann, W. J., & Dimmroth, K. (2017).** Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany. *Media and Communication*, 5(1), 7–16.
- Steiner, F., Grzymek, V., & Steiner, F. (2020).** Digital Sovereignty in the EU (Vision Europe). Bertelsmann Stiftung.
- SVRV. (2017).** Digitale Souveränität Gutachten des Sachverständigenrats für Verbraucherfragen [Digital Sovereignty Report of the German Expert Council for Consumer Affairs]. Sachverständigenrat für Verbraucherfragen [Expert Council for Consumer Affairs].
- T Timmers, P. (2019).** Strategic Autonomy and Cybersecurity. *EU Cyber Direct – Supporting the EU Cyber Diplomacy*. https://eucyberdirect.eu/content_research/strategic-autonomy-and-cybersecurity/
- V von der Leyen, U. (2020).** Shaping Europe’s digital future: Op-ed by Ursula von der Leyen, President of the European Commission. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260
- Voss, A. (2020).** A manifesto for Europe’s digital sovereignty and geo-political competitiveness. <https://www.axel-voss-europa.de/wp-content/uploads/2020/01/AVoss-Digital-Manifesto-2020-english-1.pdf>
- W Wu, T. S. (1997).** Cyberspace Sovereignty – The Internet and the International System. *Harvard Journal of Law and Technology*, 10(3), 647–666.
- Z Zuboff, S. (2019).** The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

The Author

Dr Julia Pohle is a senior researcher at the WZB Berlin Social Science Center. Her research and publications focus on national Internet policy and global Internet governance processes. Julia is actively involved in debates on digital sovereignty and internet governance and serves as a speaker, moderator and organiser at international conferences (e. g. IGF, UN, UNESCO, EU Commission, IGF-D). Since 2015, she has been a member of the Steering Committee of the German Internet Governance Forum (IGF-D).



Striving to strengthen digital sovereignty has become a cornerstone of German and European digital policy. But what is actually meant by this concept? What policies are associated with it? Is it actually a political-strategic concept or rather a buzzword? In this paper, the manifold meanings of the concept of digital sovereignty in Germany and Europe are intensively broken down and critically examined.