*This is an Accepted Manuscript of a book chapter published in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (Hart 2021), https://www.bloomsburyprofessional.com/uk/data-protection-beyond-borders-9781509940677/*

# Digital Sovereignty in the EU: Challenges and Future Perspectives

Edoardo Celeste

School of Law & Government, Dublin City University

## I. Introduction

In October 2019, at the annual Digital Summit in Dortmund, the German Federal Minister for Economic Affairs Peter Altmaier, in partnership with the French Minister of Finance Bruno Le Maire, officially launched Gaia-X, the project of a European data infrastructure.[1] In an economy currently dominated by American and Chinese tech giants, Germany and France are investing in the creation of a federated cloud 'made in Europe'.[2] According to the supporters of this initiative, only in this way will Europe eventually regain its 'digital sovereignty' and ultimately preserve its values in the digital ecosystem.[3]

[1] Bundesministerium für Wirtschaft und Energie, 'Pressemitteilung zur deutsch-französischen Zusammenarbeit für eine sichere und vertrauenswürdige Dateninfrastruktur' <https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2019/20191029-pressemitteilung-zur-deutsch-franzoesischen-zusammenarbeit-fuer-eine%20sichere-vertrauenswuerdige-dateninfrastruktur.html> accessed 21 May 2020. On the mission and activities of the Digital Summit, see 'Digital-Gipfel' <https://www.de.digital/DIGITAL/Redaktion/DE/Dossier/digital-gipfel.html> accessed 21 May 2020.

[2] Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (2019) <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=>; Federal Ministry for Economic Affairs and Energy (BMWi), 'Digital Sovereignty in the Context of Platform-Based Ecosystems' (2019) <https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digital-sovereignty-in-the-context-of-platform-based-ecosystems.pdf?__blob=publicationFile&v=7>.

[3] Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2); see also Bundesministerium für Wirtschaft und Energie, 'GAIA-X' <https://www.bmwi.de/Redaktion/DE/Dossier/gaia-x.html> accessed 22 May 2020.

Back in 2017, French President Emmanuel Macron stressed the importance of regaining sovereignty in the digital sector as one of the key policies to 'refound' the EU.[4] German Chancellor Angela Merkel, in her speech at the Internet Governance Forum 2019, reiterated the centrality of digital sovereignty in the European digital policy agenda, but at the same time earnestly highlighted that this concept may have various meanings and be interpreted in different ways.[5] As other neologisms combining the adjective 'digital' with a previously existing and well-established concept, the expression 'digital sovereignty' presents a high evocative power and, simultaneously, scarcely defined contours.[6] At first sight, it could look like an oxymoronic expression. The adjective 'digital' evokes the idea of a borderless virtual space, an un-territorial[7] or post-territorial[8] dimension where states, 'weary giants of flesh and steel, […] have no sovereignty'.[9] Sovereignty instead is a concept that historically emerged and evolved in association with the idea of territory, people and power.[10]

This chapter aims to reconstruct the meaning of digital sovereignty, and to understand the significance, rationale and challenges of this concept as a core value inspiring recent policy in the EU. The chapter will be articulated in two parts. The first part conceptualises the notion of digital sovereignty. In particular, it analyses the historical evolution of the concept of sovereignty in general, contextualises its application in the digital ecosystem, and provides a definition of 'digital sovereignty'. The second part of the chapter then looks at how this concept has been articulated in the EU. It explains that the rationale underlying the idea of digital sovereignty in the EU lies in the need to preserve the European DNA of values and rights. European data are mostly processed by foreign companies and stored outside the EU. This circumstance poses serious risks in terms of potential fundamental rights violations. The chapter thus illustrates a series of initiatives

---

[4] 'Les 6 piliers du plan de Macron pour "refonder l'Europe"' (*L'Obs*, 26 September 2017) <https://www.nouvelobs.com/politique/20170926.OBS5171/les-6-piliers-du-plan-de-macron-pour-refonder-l-europe.html> accessed 9 July 2020.

[5] 'Rede von Bundeskanzlerin Angela Merkel zur Eröffnung des 14. Internet Governance Forums 26. November 2019 in Berlin' <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> accessed 22 May 2020.

[6] Cf. Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 International Review of Law, Computers & Technology 76.

[7] See Jennifer Daskal, 'The Un-Territoriality of Data' [2015] Yale Law Journal 326.

[8] See Paul De Hert and Johannes Thumfart, 'The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies' (2018) 4 Brussels Privacy Hub Working Paper <https://papers.ssrn.com/abstract=3228388> accessed 22 May 2020.

[9] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996) <https://www.eff.org/cyberspace-independence> accessed 11 December 2018.

[10] FH Hinsley, *Sovereignty* (2nd ed, Cambridge University Press 1986) 88; for a historical perspective on the concept of sovereignty see also Jens Bartelson, *A Genealogy of Sovereignty* (Cambridge University Press 1995); for a comprehensive overview of the contemporary meaning of the notion of sovereignty, including in the context of the digital ecosystem, see Richard Rawlings, Peter Leyland and Alison Young (eds), *Sovereignty and the Law: Domestic, European and International Perspectives* (Oxford University Press 2013).

emerged at member state and Union level that seek to regain digital sovereignty in the EU. The last section finally highlights the risks associated with this tendency, warning that digital sovereignty claims can easily degenerate into forms of sovereigntism. It will be argued that EU rights and values can continue to be uphold without resorting to a counterproductive arm-wrestling with foreign countries, by respecting the principles of international comity, peacefully cooperating and respecting pluralism.

## II. Conceptualising digital sovereignty

In the existing literature as well as in policy documents, the concept of digital sovereignty has not received a univocal definition. This is partially due to the fact that the notion of sovereignty itself has evolved throughout history and has never been definitively defined.[11]

### A. What is sovereignty?

The core idea of sovereignty lies in the concepts of supremacy of power over a territory and independence.[12] In Latin, *superanus* literally meant who stands 'above'.[13] In the Middle Ages, sovereign was the person who held supreme power over a territory. However, at that time, sovereignty was not synonymous of absolute power, but only denoted a 'relative pre-eminence'.[14] Paradigmatic examples are those of the kings of England, who were at the same time vassals of the kings of France, and of the catholic bishops, whose jurisdiction trumped that of temporal authorities in religious matters.[15]

Subsequently, the concept of sovereignty constantly evolved. Sovereignty gradually started to denote a form of power that is not only supreme, but also absolute, original, indivisible and inalienable.[16] Traditionally, the Peace of Westphalia, terminating the Thirty Years War in 1648, marks the start of the modern idea of sovereignty, intended as

---

[11] See Hent Kalmo and Quentin Skinner (eds), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (Cambridge University Press 2010).

[12] See Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal 328.

[13] 'Sovereign, n. and Adj.' <https://www.oed.com/view/Entry/185332#eid21519750> accessed 26 May 2020.

[14] 'sovranità', *Dizionario di filosofia Treccani* (2009) <http://www.treccani.it//enciclopedia/sovranita_(Dizionario-di-filosofia)> accessed 26 May 2020; on the possibility of conceiving a form of sovereignty in the Middle Ages, cf. Francesco Maiolo, *Medieval Sovereignty: Marsilius of Padua and Bartolus of Saxoferrato* (Eburon 2007) 19 ff.; on the same point, talking of 'proto-sovereignty' and with reference to the Renaissance, see also Bartelson (n 14) 88 ff.

[15] Further on the point see George W White, *Nation, State, and Territory: Origins, Evolutions, and Relationships* (Rowman & Littlefield 2004) 124 ff; Joseph Canning, *Ideas of Power in the Late Middle Ages, 1296-1417* (Cambridge University Press 2014).

[16] A major impulse in this direction was brought by Bodin: see CH McIlwain, 'Sovereignty Again' [1926] Economica 253; see also Stewart Motha, 'Sovereignty', *The New Oxford Companion to Law* (Oxford University Press 2008) <https://www.oxfordreference.com/view/10.1093/acref/9780199290543.001.0001/acref-9780199290543-e-2052> accessed 25 May 2020; Hinsley (n 10) ch 3.

supreme authority of a state within its own territory and independence from the interference of other sovereign entities.[17]

The following centuries saw philosophers debating on the questions of who or which entity really holds sovereignty, and what the limits of their supreme power are.[18] The apex of the conceptual parabola of the concept of sovereignty was also the prelude of its descending phase. Before World War Two, the German legal theorist Carl Schmitt still regarded the essence of sovereignty as lying in the power to suspend statutory guarantees and declare the state of emergency: sovereign was the entity who takes the 'decision on the exception'.[19] The atrocities of the first half of the Twentieth century inexorably led to a rethinking of the idea of sovereignty.[20] The sovereign state could no longer risk to be totally unbound, but should be subject to internal and external limitations.[21]

### B. Sovereignty in the digital society

The decline – or one would more correctly say, the evolution – of the traditional conception of sovereignty has undoubtedly been exacerbated by the advent of digital technologies. In 1996, John Perry Barlow published the famous *Declaration of the Independence of Cyberspace*, championing the idea that the virtual world was merely the 'home of Mind', a new sanctum sanctorum of culture and freedom where states could not exercise their power, and their legal system would not apply.[22] The traditional idea of state sovereignty, intended as supreme power of the state over a territory and independence from other sovereign entities, apparently found an insurmountable limit in the intangibility of the new space that digital technologies created. Cyberspace itself allegedly emerged as an independent, sovereign entity.[23]

In reality, as the scholarship promptly remarked, this cyber-anarchist view was merely utopian.[24] First of all, digital technologies still relied on physical apparatuses, tangible

---

[17] Daniel Philpott, 'Sovereignty' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (2016) <https://plato.stanford.edu/archives/sum2016/entries/sovereignty/> accessed 25 May 2020.

[18] For a comprehensive and concise overview, see Philpott (n 17); see also Dieter Grimm, *Sovereignty: The Origin and Future of a Political and Legal Concept* (Columbia University Press 2015) chs 2 and 3.

[19] Stewart Motha, 'Sovereignty', *The New Oxford Companion to Law* (Oxford University Press 2008) <https://www.oxfordreference.com/view/10.1093/acref/9780199290543.001.0001/acref-9780199290543-e-2052> accessed 26 May 2020.

[20] See Philpott (n 17).

[21] On the point see Philpott (n 17); see also Rawlings, Leyland and Young (n 10); Anne Peters, 'Humanity as the A and Ω of Sovereignty' (2009) 20 European Journal of International Law 513.

[22] Barlow (n 9).

[23] For a comprehensive, but concise overview of the scholarship in favour of cyberspace sovereignty see Dan Jerker B Svantesson, 'Sovereignty in International Law: How the Internet (Maybe) Changed Everything, but Not for Long' (2014) 8 Masaryk University Journal of Law and Technology 137, 144 ff.

[24] See Tim Wu, 'Cyberspace Sovereignty? – The Internet and the International System' (1997) 10 Harvard Journal of Law & Technology 647; Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65 The University of Chicago Law Review 1199; Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2008).

properties that the 'giants of flesh and steel' could physically control.[25] Secondly, nation states soon understood that the Internet was not *terra nullius*. Nothing prevented them from regulating the conduct of individuals over Internet, and that this was even desirable, not to say necessary.

As seen in the previous chapters of this book, recent examples include the scope of application of the General Data Protection Regulation (GDPR) or the US Cloud Act.[26] Article 3(2) GDPR provides that the new pan European data protection legislation applies to data controllers and processors, which are *not* established in the EU, if they process data related to the offer of goods or services to data subjects in the EU or monitor the behaviour of individuals located in the EU.[27] The US Cloud Act empowers law enforcement authorities to request data in the 'possession, custody and control' of a US company, notwithstanding the fact that such information may be stored in servers located outside the US.[28] These two pieces of legislation demonstrate how nation states found alternative ways to exercise their sovereign power, which are not primarily based on the concept of territory.

Interestingly, this phenomenon of adaptation of the notion of territorial sovereignty to a globalised and borderless world has never been described in terms of digital sovereignty, nor has it been considered as a fully legitimate extension of the sovereign power of the state over the digital territory. The legal scholarship persists in studying this centrifugal tendency as a form of regulatory overreaching or jurisdictional trawling.[29] As we have seen in the previous chapters of this book, the traditional indissoluble bond between sovereignty and territory rightly imposes to categorise this phenomenon as *extra*-territorial.[30] Interestingly, De Hert and Thumfart regarded it as a form of 'hyper-sovereignty', qualifying it as a reaction to cyberanarchy. This phenomenon would entail an exorbitant use of sovereign power, generating what Lessig called 'competition among sovereigns',[31] and unavoidably leading to an erosion of the rule of law both at national and international level.[32] Although the authors in this case recognise a scission between digital ecosystem and territory, their *post*-territorial conception does not lead to

[25] What Svantesson calls 'sovereignty over the technology' in opposition to 'sovereignty over conduct'. See Svantesson, 'Sovereignty in International Law' (n 23).

[26] On these respective topics, see in this book the chapters by Fabbrini and Celeste, Lynskey and Smith.

[27] See also Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5 International Data Privacy Law 235.

[28] See also Halefom H Abraha, 'How Compatible Is the US "CLOUD Act" with Cloud Computing? A Brief Analysis' [2019] International Data Privacy Law.

[29] See Dan Jerker B Svantesson, 'Internet & Jurisdiction Global Status Report 2019' (2019) <https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report>.

[30] In this book, see Fabbrini and Celeste, ch 2.

[31] Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books 2006) ch 15.

[32] De Hert and Thumfart (n 8).

reconceptualise the core tenets of contemporary sovereignty, and especially its rooting in a territory.

This conceptual inability to severe the link between state sovereignty and territory was certainly one of the factors that pushed nation-states to find a natural alternative to solve the dilemma of regulating the digital society in the re-territorialisation of the digital ecosystem. For example, recently, as Quinn examined in detail in this book, the CJEU demanded Google to delist search results from its website by virtue of a person's right to be forgotten, and to limit such a delisting to the territory of the EU, encouraging the use of geo-blocking technologies.[33] Erecting frontiers in a space that originally emerged as borderless has appeared as a sound solution to forestall the risk of anarchy, and at the same time to prevent one or few powerful states from imposing a digital monarchy or oligarchy:[34] a phenomenon that from a cyber-libertarian point of view is negatively denoted as Internet balkanisation.[35]

Recently, this tendency of reasserting boundaries in the digital ecosystem has been accompanied by states' attempts to regain control over data and digital infrastructures. Several states have adopted data localisation laws, requiring controllers to physically store data within the territory of the state.[36] New initiatives have emerged to create national or regional digital infrastructures, as shown in the Gaia-X example presented in the introduction.[37] Interestingly, it is only in this specific context that explicit claims to digital sovereignty emerged. States, particularly in Europe, are invoking this concept to trigger centripetal and centralist trends on data and digital infrastructures, in this way seeking to regain independence from foreign service providers and increase their capabilities of controlling these strategic assets.

## C. Defining digital sovereignty

As the concept of sovereignty has evolved over time and its meaning has never been set in stone, a canonical definition of digital sovereignty similarly does not exist. The emergence of this expression is quite recent – no academic articles including this word

[33] See *Google Spain v APED* [2014] ECJ C-131/12, ECLI:EU:C:2014:317; *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECJ C-507/17, ECLI:EU:C:2019:772. See also, in this volume, Fabbrini and Celeste, ch 2, Pollicino, ch 6, and Quinn, ch 4.

[34] See Lessig (n 31) 302 ff, who talks of 'no law rule' and 'one law rule'.

[35] Cf. Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (Polity 2017).

[36] See Edoardo Celeste and Federico Fabbrini, 'Competing Jurisdictions: Data Privacy Across the Borders' in Grace Fox, Theo Lynn and Lisa van der Werff (eds), *Data Privacy and Trust in Cloud Computing* (Palgrave 2020); John Selby, 'Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?' (2017) 25 International Journal of Law and Information Technology 213; Neha Mishra, 'Data Localization Laws in a Digital World: Data Protection or Data Protectionism?' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2848022 <https://papers.ssrn.com/abstract=2848022> accessed 8 November 2019.

[37] See also *infra* in this chapter.

have been found before 2011 – and it is still not common in the academic milieu.[38] Digital sovereignty appears as the last offspring of the family of concepts applying the notion of sovereignty to the technological world. The expression 'technological sovereignty' already emerged in the 1960's.[39] 'Data sovereignty' is the most used concept of the family both in academic and commercial articles, but it now appears to be conceived as a component of the notion of digital sovereignty.[40] This trend is not surprising, as our vocabulary changes following the evolution of technology, and reflects the relative importance that these innovations play within society.[41]

In the documents presenting the project Gaia-X published by the German Federal Ministry for Economic Affairs and Energy, digital sovereignty is depicted as 'an aspect of general sovereignty',[42] and is defined as:

> the 'possibility of independent self-determination by the state and by organisations' with regard to the 'use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result.'[43]

Data sovereignty would then be at its turn an integral part of the concept of digital sovereignty, denoting the ability of having 'complete control over stored and processed data and also the independent decision on who is permitted to have access to it'.[44]

If one compares these definitions with the core elements of modern sovereignty, intended as supreme power of the state over a territory and its independence from external entities, one can notice a series of similarities and differences. In terms of general architecture, digital sovereignty does not subvert the core tenets of traditional sovereignty, preserving its conceptual genes.[45] Yet, the concept of digital sovereignty articulates the notion of sovereignty in the context of the digital ecosystem. The definition quoted above does not explicitly mention the idea of territory. Digital sovereignty denotes a form of control over

---

[38] For a discourse analysis of the literature on digital sovereignty see Stephane Couture and Sophie Toupin, 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?' (2019) 21 New Media & Society 2305.

[39] Couture and Toupin (n 38).

[40] Couture and Toupin (n 38); on the use of the concept of data sovereignty as an aspect of digital sovereignty see Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2).

[41] See, e.g., in relation to the concept of digital constitutionalism, Edoardo Celeste, 'The Scope of Application of Digital Constitutionalism. Output from an Empirical Research' (Nexa Research Papers 2017) Nexa Research Papers <https://nexa.polito.it/nexacenterfiles/E.%20Celeste%20-%20Research%20Paper.pdf>.

[42] Federal Ministry for Economic Affairs and Energy (BMWi), 'Digital Sovereignty in the Context of Platform-Based Ecosystems' (n 2) 6.

[43] Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2) 7.

[44] Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2) 7.

[45] Cf. Celeste, 'Digital Constitutionalism' (n 6).

digital assets, which can be material and immaterial entities, thus potentially 'located' in a space that transcends physical boundaries. Moreover, digital sovereignty is not only a prerogative of states, but also of private 'organisations' that are vested with this power. States alone cannot cope with the challenges of a globalised world; regional and international organisations, such as the EU, necessarily emerge to complement states' functions.[46] Finally, although the element of 'control' is still rooted in the concept of digital sovereignty, particular emphasis is placed on the ability to be 'independent' from external interference. In the Gaia-X documents, for instance, digital sovereignty is defined as '*independent self*-determination'. The prominence given to this aspect of sovereignty should not be underestimated because it reflects the peculiar context in which the concept of digital sovereignty has emerged: the European appeal to regain independence in the digital field. The next section will analyse how claims to digital sovereignty have surfaced in the EU and what their rationale is.

## III. Digital sovereignty in the EU

Today, digital technologies are an integral part of the everyday life of individuals, companies and institutions in Europe, but the market for digital products and services is dominated by American and Chinese multinational corporations.[47] Multiple risks are identified in the European inability to fully control its data and digital infrastructures. Regaining sovereignty on its portion of the digital ecosystem is seen in the EU as a potential solution to preserve its unique DNA of rights and values. To this purpose, a series of initiatives have emerged both at member states and union level. However, as we will see in the following sections, this phenomenon risks degenerating in an economically and legally counter-productive sovereigntist arm-wrestling.

### A. Preserving the European DNA

Digital sovereignty claims have originally materialized in Europe in response to a perceived excessive role of foreign technology companies.[48] What is traditionally defined as 'external' sovereignty, the capability of a state to exercise its power without interference of other entities, is perceived under threat in the European digital society. Products and services offered by non-European multinationals dominate the market, consequently imposing their values and rules. European individuals and institutions are left to the mercy of technology firms from China and the US.

---

[46] See, e.g. Petra Dobner and Martin Loughlin (eds), *The Twilight of Constitutionalism?* (Oxford University Press 2010) pt 1; Anne Peters, 'Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures' (2006) 19 Leiden Journal of International Law 579.

[47] In relation to the cloud sector, see, eg, Will Bedingfield, 'Europe Has a Plan to Break Google and Amazon's Cloud Dominance' [2020] *Wired UK* <https://www.wired.co.uk/article/europe-gaia-x-cloud-amazon-google> accessed 5 June 2020.

[48] See Pierre Bellanger, *La souveraineté numérique* (Stock 2014).

This condition is regarded negatively for a series of reasons, both generally and specifically related to the two countries dominating the technological sector: China and the US. First of all, data and digital infrastructures are seen as assets of critical importance for the European economic development.[49] Therefore, heavily relying on non-European service providers could increase the risk of an excessive dependency on those countries.[50] A consideration that today, in the current trade war between the US and China, seems to be more concrete than ever.[51]

Secondly, foreign countries may not offer an adequate level of protection to European personal data. According to the GDPR, this is one of the conditions among others authorising the transfer of European personal data to third countries.[52] However, looking beyond this normative requirement, even in these cases, European personal data could be exposed to risks. As a paradigmatic example, one can mention the existence of the US mass surveillance programme unveiled by Edward Snowden in 2013, which also involved data of millions of European users.[53] A factor that certainly enhanced the level of suspicion that EU member states currently harbour towards the level of data protection offered by the US.[54] China, on the other side, is generally mistrusted as a non-democratic country, and the recent adoption in 2017 of a new National Intelligence Law obliging Chinese companies to collaborate with Chinese intelligence agencies certainly does not help.[55] Finally, the Cambridge Analytica scandal implicating Facebook in 2018 also illustrates that a concrete threat for data protection could come not only from foreign law enforcement and intelligence agencies, but also from private corporations.[56]

Thirdly, and more generally, a heavy reliance on foreign service providers may expose Europeans to potential fundamental rights infringements. Before the *Schrems* decision, for instance, where the Court of Justice of the EU (CJEU) invalidated the agreement allowing the transfer of EU personal data to selected American companies, EU data

---

[49] See European Commission, 'A European Strategy for Data' (2020) COM(2020) 66 final <https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf>.

[50] See Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2).

[51] For a comprehensive view on the latest news on the issue, see 'US-China Trade Dispute' (*Financial Times*) <https://www.ft.com/us-china-trade-dispute> accessed 5 June 2020.

[52] For a succint, but comprehensive overview see Celeste and Fabbrini (n 36).

[53] See Ioanna Tourkochoriti, 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-E.U. in Data Privacy Protection' (2014) 36 University of Arkansas at Little Rock Law Review 161.

[54] See Edoardo Celeste and Federico Fabbrini, 'Targeted Surveillance: Can Privacy and Surveillance Being Reconciled?' in Sergio Carrera, Deirdre Curtin and Andrew Geddes (eds), *20 Year Anniversary of the Tampere Programme. Europeanisation Dynamics of the EU Area of Freedom, Security and Justice* (European University Institute 2020).

[55] See Yuan Yang, 'Is Huawei Compelled by Chinese Law to Help with Espionage?' *Financial Times* (5 March 2019) <https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0> accessed 1 December 2019; Celeste and Fabbrini (n 36).

[56] See Patrick Greenfield, 'The Cambridge Analytica Files: The Story so Far' *The Guardian* (25 March 2018) <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far> accessed 30 April 2019.

subject did not have any right to judicial redress before US courts in case of infringement of their data protection rights.[57]

From these considerations, it is possible to argue that the main rationale behind digital sovereignty claims in the EU lies in the willingness to preserve European core values, rights and principles. By invoking control on personal data and digital infrastructures, the EU is seeking to maintain its fundamental values of respect for democracy and human rights unaltered vis-à-vis the challenges of the global digital society.[58] In a communication released in February 2020, the EU Commission stressed the difference between the American, Chinese and European strategy in the context of the data economy. The US would be characterised by a predominant role of private actors; in China, the government would play an incisive oversight role; the 'European way', conversely, would combine the need to preserve a free-flow of data and competition among economic players with high standards of protection in terms of privacy, security, ethics and fundamental rights in general.[59]

According to the Commission, this can be achieved through the creation of a 'European data space', where an adequate level of digital infrastructures allows for the processing a data-driven economy, and EU law and its fundamental rights are respected and enforced effectively.[60] The next paragraph will explore which measures have been concretely suggested to be implemented both at national and EU level.

### B. Member states and Union initiatives

Measures invoked in the name of digital sovereignty share the exercise of a centripetal force on data and digital infrastructures by states or supranational organisations. At first sight, they could be seen as the opposite of extraterritorial measures.[61] States do not seek to extend their jurisdiction on data or digital infrastructures located abroad by stretching the scope of their regulation; they rather attempt to reattract such data and digital infrastructures within their classical jurisdictional boundaries by requiring their 'physical' return within their territories.

---

[57] *Schrems* [2015] ECJ C-362/14, ECLI:EU:C:2015:650; see David Cole, Federico Fabbrini and Stephen J Schulhofer (eds), *Surveillance, Privacy, and Transatlantic Relations* (Hart Publishing 2017) ch 11.

[58] See European Commission (n 49); see also Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019) para 4.

[59] European Commission (n 49) 3.

[60] European Commission (n 49) 4–5; cf. Selby (n 36), who considers local law enforcement as one of the drivers of digital sovereignty claims.

[61] See Bertrand de La Chapelle and Paul Fehlinger, 'Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) <https://www.cigionline.org/sites/default/files/gcig_no28_web.pdf> accessed 8 June 2020.

A paradigmatic example is represented by so-called data localisation, or data residency initiatives, whereby a state or a supranational organisation requires personal data to be stored within its territory.[62] In 2014, for instance, the CJEU in *Digital Rights Ireland* invalidated the Data Retention Directive.[63] The Directive provided for the retention of communications metadata for law enforcement purposes. In other words, service providers were required to store all data relating to one person's communications, such as time, location or receiver of a phone call, but excluding its content, for a specific amount of time in order to allow law enforcement authorities to access them for the prosecution of a criminal offence. The CJEU invalidated the Data Retention Directive on a series of grounds, including its failure to require communications providers to store metadata in the EU.[64] Article 8 of the Charter of Fundamental Rights of the EU enshrines a right to data protection, and at paragraph 3 explicitly vests national data protection authorities with the duty to ensure compliance with this right. According to the CJEU, the power of these oversight agencies would be irremediably restricted if telecommunication providers were able to store metadata outside the EU, and thus beyond their jurisdiction. Hence, the necessity, derived *a contrario* from the judgment of the CJEU, to store metadata with the EU territory.

*Digital Rights Ireland* exclusively concerned the storage of users' metadata for law enforcement purposes. There is no absolute obligation to store personal data in the EU; personal data can be freely transferred outside the EU, subject to specific rules.[65] However, in *Digital Rights Ireland*, the CJEU balanced the necessity to preserve such a relatively free-flow of data with the need to ensure a high level of protection of this specific processing requirement. In particular, the CJEU's solution was justified by the particular risks that storing a significant amount of metadata outside the EU may entail in terms of security and protection, such as risks of abuse, unlawful access and use.[66]

A similar sectoral approach was adopted in other countries, both in the EU and beyond, for analogous reasons.[67] In the EU, many member states require financial data to be stored on the national soil; some of them impose similar obligations on public institutions.[68] However, in contrast to these balanced solutions, other states have preferred more holistic data localisation regimes.[69] In 2014, for instance, the Russian Federation passed a bill requiring the compulsory storage of all citizens' personal data collected by electronic

---

[62] Cf. Selby (n 36) 214.

[63] *Digital Rights Ireland* [2014] ECJ Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238; for an analysis of the case, see Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15 European Constitutional Law Review 134.

[64] *Digital Rights Ireland* (n 63) para 68.

[65] See GDPR, art. 44 ff.

[66] *Digital Rights Ireland* (n 63) paras 66–68.

[67] See Anupam Chander and Uyên P Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677; see also Selby (n 36).

[68] See Selby (n 36) 226 .

[69] See Selby (n 36) 215.

communication providers within the territory of the state.[70] Similarly, Chinese law imposes to store within the national territory all personal data collected by critical information infrastructures, such as healthcare, financial institutions, energy and transport companies.[71]

Similar wide-ranging data localisation measures have never been taken in Europe on a permanent basis. In 2013, in the aftermath of the Snowden revelations, the conference of the German national data protection authorities suspended issuing authorisations for data transfers from Germany to non-EU countries.[72] More recently, in 2019, the Commissioner for Data Protection and Informational Liberty of the Land of Hessen, in central Germany, temporarily prohibited the use of Microsoft Office 365 by schools.[73] The national data protection authority claimed that Microsoft's decision to store data outside the EU would have exposed personal information related to Hessian children to the risk of being accessed by US law enforcement authorities.[74] The Microsoft ban, therefore, would have been justified to preserve the state's digital sovereignty by ensuring that the level of protection accorded to data processed by Microsoft be in line with European and German fundamental rights.[75]

The recent decision of the Hessian data protection is a paradigmatic example of the challenges and the implications of claiming digital sovereignty in the EU. Non-European corporations often offer state-of-the-art products and services used by millions of users in the Union. Guaranteeing a high level of data protection within the EU by physically storing data in the territory of the Union implies that non-European companies renounce to use their digital infrastructures located abroad. However, in this case, the main quandary is whether existing digital infrastructures in the EU are able to satisfy its internal

---

[70] See W Kuan Hon and others, 'Policy, Legal and Regulatory Implications of a Europe-Only Cloud' (2016) 24 International Journal of Law and Information Technology 251; Selby (n 36).

[71] On the point see Selby (n 36) 225 ff.

[72] President of the federal and national data protection authorities 2013, 'Press Release. Conference of Data Protection Commissioners Says That Intelligence Services Constitute a Massive Threat to Data Traffic between Germany and Countries Outside Europe' (2013) <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile>; See Chander and Lê (n 67) 692.

[73] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 'Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen' (*Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*, 9 July 2019) <https://datenschutz.hessen.de/service> accessed 30 November 2019; see also Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 'Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen' (*Der Hessische Beauftragte für Datenschutz und Informationsfreiheit*, 2 August 2019) <https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen> accessed 30 November 2019, in which the Hessian data protection authority lifted its ban after an intense phase of dialogue with Microsoft.

[74] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 'Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen' (n 73) para 2.

[75] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 'Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen' (n 73) para 2.

demand. Many initiatives emerged both at national and Union level, by advocating the creation of such an infrastructure, speak of the inadequacy of existing resources in the EU.[76] In this context, one can mention the idea – proposed since 2011 – of an EU-only cloud or even a 'Schengen' virtual area.[77] In 2016, the European Commission launched the European Cloud Initiative as a key component of its Digital Single Market Strategy.[78] This project would entail the creation of a European Open Science Cloud, a secure cloud infrastructure for researchers, and a European Data Infrastructure, which would provide the underlying super-computing solutions.

Some member states have long tried to put in place national digital infrastructures. In 2011, the French government launched the project of a 'sovereign cloud', Andromède, subsequently giving origin to two competing platforms, Cloudwatt, managed by Orange, and Numergy, led by SFR.[79] In 2013, Deutsche Telekom presented a project to create an 'Internetz', a German-only Internet routing all traffic data nationally.[80] More recently, the launch of the Franco-German Gaia-X project, which advocates the creation of a pan-European federated cloud infrastructure, witnesses an acknowledgement of the necessity to overtaking a parochial approach and joining the forces at EU level to deliver a broader, more scalable, and consequently potentially more successful, digital infrastructure.[81] Such a federated approach seems also to be the solution recently advocated by the EU Commission in its 2020 communication on a EU strategy for data.[82] The European data space will be the result of a plurality of EU-wide interoperable digital ecosystems, each one covering a critical sector of the European economy.[83] To achieve this result, the Commission does not only plan to invest a significant amount of resources to build the necessary infrastructure in the next decade, but also aims to introduce a coherent legislative package that would complement the existing regulatory framework for data, without however imposing a rigid *ex ante* regulation.[84]

### C. The risk of digital sovereigntism

In Europe, digital sovereignty claims have explicitly emerged in relation to a specific number of initiatives. However, if one takes a functional approach, looking at the ultimate

[76] See also European Commission (n 49).

[77] See C Kuner and others, 'Internet Balkanization Gathers Pace: Is Privacy the Real Driver?' (2015) 5 International Data Privacy Law 1; Hon and others (n 70).

[78] European Commission, 'European Cloud Initiative - Building a Competitive Data and Knowledge Economy in Europe' (2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0178&from=EN>.

[79] See Bedingfield (n 47).

[80] See Hon and others (n 70).

[81] See Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2).

[82] European Commission (n 49) 16.

[83] European Commission (n 49) 12, 16.

[84] European Commission (n 49) 12.

aim of digital sovereignty claims, which is to regain control and independence in the management of the digital ecosystem, it is possible to identify a series of other mechanisms that would contribute to (re)affirm the European digital sovereignty. Chander and Lê, for example, consider the EU data protection rules limiting the transfer of personal data to third countries as a claim of digital sovereignty, even though this is not an explicit objective of the GDPR.[85] Looking beyond the EU, Fischer in this book has analysed the US attempt to adopt a federal data privacy law.[86] This bill certainly represents an attempt to respond to the Cambridge Analytica scandal and to avoid a scenario of legislative fragmentation in the US after the recent enactment of privacy legislation by California. However, one may also argue that it aims to reaffirm the American privacy values and ultimately its digital sovereignty. The broad scope of application of the GDPR and the introduction of harsh fines in case of violation of data protection rules pushed American companies to proactively embrace the new European standards.[87] This further example of Brussels effect in the field of data protection may be arguably read from an American standpoint as a form of imperialism, and, at any rate, as a de facto erosion of digital sovereignty.[88]

Interestingly, following this line of arguments, even an apparent expression of legislation with extraterritorial reach such as the US CLOUD act, commented by Smith in this book, may be regarded as a form of exercise of digital sovereignty.[89] The US would aim to reassert their control over data which American multinational companies store abroad in order to comply with foreign data protection law. And of course, in the same way, one may contend that the broad scope of application of the GDPR, encompassing also companies not established in the EU territory, is equally to be regarded as a corollary of European digital sovereignty.[90]

Paradoxically, therefore, this functional interpretation of digital sovereignty leads to conflate centripetal and centrifugal pressures in a single phenomenon: extraterritoriality and localisation become two sides of the same coin. Digital sovereignty emerges as a useful lens to interpret this complex mix of apparently opposite trends. However, by embracing this interpretation, it is apparent that the element of territory, which was central to the traditional notion of sovereignty, loses its centrality. All forms of digital

---

[85] Chander and Lê (n 67).

[86] See Ch 3.

[87] See Michael L Rustad and Thomas H Koenig, 'Towards a Global Data Privacy Standard' (2019) 71 Florida Law Review 365.

[88] On the Brussels effect in the field of data protection, see Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020) ch 5; on the notion of data protection imperialism see Federico Fabbrini and Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 German Law Journal 55; see also Dan Jerker B Svantesson, 'The Google Spain Case: Part of a Harmful Trend of Jurisdictional Overreach' (2015) EUI Working Papers <http://cadmus.eui.eu//handle/1814/36317> accessed 15 January 2020; cf. Rustad and Koenig (n 87) who also analyse an opposite 'D.C. effect'.

[89] See Ch 8.

[90] Cf Quinn, Ch 4.

sovereignty aim to gain and maintain control on the digital ecosystem. The reference to a territory becomes only one of various mechanisms that states and regional organisations may use to affirm their jurisdiction over sectors of the digital world.

Overtaking the traditional anchoring to the territory, digital sovereignty may contemplate the co-existence of a plurality of sovereignties within the same physical space. This apparent oxymoron is explained by the fact that digital sovereignty may use the territory as one of the mechanisms to be asserted as much as may it resort to other reference points, such as the connection with a user located in a state or the offer of goods of services to those users. This post-territorial prospective effaces the question of territorial alignment of data protection, and more broadly, digital regulation.[91] Yet, the dilemma of how to accommodate co-existing sovereignties still persists.

A series of unfettered sovereign claims would naturally tend to a state of continuous conflict in the attempt to predominate and possibly establish a scenario of 'One Law Rule'.[92] Disanchoring sovereignty from territory does not escape the question of the limitations of digital sovereignty. One needs to find a pacific and efficient way of re-composing the mosaic of sovereign claims. In line with other scholars, this paper contends that a global digital society may continue to exist, while preserving states' interests.[93] The solution lies in avoiding that digital sovereignty degenerates into a form of sovereigntism or nationalism.[94] The latter arises when digital sovereignty claims advocate unjustified forms of protectionism and isolationism.[95] Exercising an excessive centripetal force to attract data within Europe and subsidising the creation of digital infrastructures made in the EU could be legally and economically counterproductive. For example, data localisation policies may alter the global economic course by generating higher costs related to the relocation of data centres in Europe.[96] Centralising data in the EU is not always a synonym of enhanced security, since delocalisation may be a strategy to enhance system resilience and decrease the level of vulnerability.[97] Digital sovereigntism could exacerbate political and economic tensions with third states, leading to a strenuous arm-wrestling that, ultimately, would not enhance the protection of European data and foster our economy.[98]

---

[91] On the question of territorial alignment of cyberspace, see Mueller (n 35) ch 4 ff.

[92] Lessig (n 31) 305 ff.

[93] See, in particular, Woods (n 12); see also Chapelle and Fehlinger (n 61).

[94] Specifically in the context of data protection, see Fabbrini and Celeste (n 88), who articulate the tension between data protection imperialism and sovereigntism; Chander and Lê (n 66), who describe this phenomenon in terms of 'data nationalism'.

[95] See Kuner and others (n 77); Christopher Millard, 'Forced Localization of Cloud Services: Is Privacy the Real Driver?' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2605926; Celeste and Fabbrini (n 36).

[96] Mishra (n 36).

[97] Mishra (n 36).

[98] In relation to cloud computing, see Celeste and Fabbrini (n 36).

Defending the European DNA of values and rights is of utmost importance. Nevertheless, this should not nurture a form of legal-economic insularity nor should it justify a revamp of European normative imperialism overstretching the scope of application of EU law. In the global digital ecosystem, the EU should preserve its ideological genes by simultaneously considering the transnational consequences of its regulatory activity.[99] As argued by Quinn in this volume, the *Google v. CNIL* case recently decided by the CJEU went exactly in this direction, posing the fundamental questions of what would happen if the EU imposed word-wide delisting orders to search engines, and if all sovereign states exercised the same prerogative.[100] Absent a cosmopolitan solution, respecting the principles of international comity emerges as the only viable prospect.[101] In a world characterised by manifold overlapping sovereignties, the respect of regulatory choices of other countries is essential to avoid counterproductive tensions.[102] In order to reconcile multiple sovereigns in a post-territorial ecosystem, Europe should be as 'open as possible, and as closed as necessary'.[103] Only in this way will the EU preserve its unique DNA of rights and values, foster its digital economy, and pacifically prosper with its foreign allies.

## IV. Conclusion

Over the past few years, a series of initiatives has been launched in the EU in the name of digital sovereignty. Data of European citizens, companies and institutions are mostly in the hands of American and Chinese technology corporations, where they may be accessed by law enforcement and intelligence authorities of these countries. Recent scandals have shown that this situation poses significant risks in terms of potential violations of fundamental rights. Geopolitical tensions between the US and China may have considerable repercussions on the level of security and availability of digital services and infrastructures in the EU. By invoking digital sovereignty, various EU initiatives seek to exercise a centripetal force on data and digital infrastructures. Imposing to store specific types of information in the EU and promoting digital products and services made in Europe would help reacquire control of European data, and at the same time enhance the degree of independence from foreign service providers. In this way, the EU would aim to preserve its unique DNA of values and rights.

---

[99] Cf. Kuner, 'The Internet and the Global Reach of EU Law' (n 58) para F.

[100] *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* (n 33); in this volume, see Quinn at Ch 4.

[101] In this sense, Woods (n 12); Fabbrini and Celeste (n 88).

[102] On the point, see *Google LLC v CNIL* (n 32), where the CJEU demanded member states to consider the existence of different approaches to data protection and in principle limit the enforcement of the right to be forgotten to the EU territory; see also the Opinion of Advocate General Szpunar in *Google LLC v CNIL* (n 32) at 61, who highlighted the risk of having third states demanding global delisting and ultimately limiting access and circulation of information at global level.

[103] This sentence has been originally coined for the EU open research data policy. See 'Open Access - H2020 Online Manual' <https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/open-access_en.htm> accessed 17 June 2020.

Digital sovereignty is a notion emerged in the EU in relation to a specific series of initiatives. However, this chapter has shown that this concept can be used as a lens to interpret a broader phenomenon. As illustrated in the first part of this chapter, historically, the notion of sovereignty has denoted the power of the state over a territory and its independence from external actors. The advent of digital technology has accelerated the transition towards a global society where national boundaries are no longer neatly demarcated. This chapter has argued that in this post-territorial ecosystem the concept of sovereignty loses its traditional anchoring to the notion of territory. The physical location of a juridical entity becomes one of the various mechanisms to exercise state sovereignty. Multiple sovereignties can be deemed to coexist in the same context. Digital sovereignty claims can therefore take the form not only of localisation law, but also of legislation having an extraterritorial scope. From this perspective, the latter is not to be automatically condemned as imperialist because territorial boundaries are no longer the exclusive parameter to consider.

However, even this post-territorial approach does not exempt us from analysing the question of the limits of digital sovereignty. On the one hand, unfettered sovereignties produce tensions between states, and ultimately risk enhancing the likelihood of having dominant players imperially regulating vast portions of the digital ecosystem. On the other hand, exercising excessively a centripetal force on data and digital infrastructures to achieve a realignment with territorial jurisdictions may lead to forms of protectionism and isolationism. The final section of this chapter has focused in particular on this last point, warning against the risk of disguising sovereigntist policies as legitimate sovereign claims.

The global digital society is an ecosystem where, as Michaels put it, 'everything has an effect on everything'.[104] The solution advanced by this paper to accommodate multiple sovereign interests in a post-territorial world consequently pivots on the respect of the principles of international comity, pacific cooperation, and the guarantee of pluralism. In this respect, EU law still seems to be in a transition phase, uncertain on which strategy to adopt to preserve its DNA of values and principles in the digital ecosystem. Kuner rightly observes that 'EU law is still searching for a paradigm for its application to the Internet'.[105] Critiques moved to EU legislative overreaching and digital sovereigntism speak of the difficulty of finding an intermediate strategy which translates sovereign interests in a global environment.[106] However, recent developments in the case-law of the CJEU show that EU law is progressively moving in the right direction.

---

[104] Ralf Michaels, 'Territorial Jurisdiction After Territoriality' in Pieter J Slot and Mielle K Bulterman (eds), *Globalisation and Jurisdiction* (Kluwer Law International 2004) 123.

[105] Kuner, 'The Internet and the Global Reach of EU Law' (n 58) 140.

[106] See Christopher Kuner, 'Data Nationalism and Its Discontents' (2015) 64 Emory Law Journal 2089, 2098.